

FEDERAL PROSECUTION OF VIOLATIONS OF INTELLECTUAL PROPERTY RIGHTS



COPYRIGHTS, TRADEMARKS AND TRADE SECRETS

Criminal Division
Computer Crime & Intellectual Property Section

May 1997

FEDERAL PROSECUTION OF VIOLATIONS OF INTELLECTUAL PROPERTY RIGHTS

(COPYRIGHTS, TRADEMARKS AND TRADE SECRETS)

May 1997
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice
Washington, D.C.

PREFACE

Over the past two decades, systematic infringement of intellectual property rights has become of increasing concern to American businesses, artists and authors. Recently, the problem has been growing much worse. The proliferation of computers and computer networks has made the illegal reproduction and distribution of protected material much easier to accomplish and more difficult to police. The federal law enforcement community has responded to this problem by promoting the enactment of new laws or the reform of existing laws which prohibit trafficking in counterfeit goods (18 U.S.C. § 2320), reproducing or distributing copyrighted works (18 U.S.C. § 2319), and stealing trade secrets (18 U.S.C. §§ 1831 *et. seq.*). We have also sought to strengthen laws protecting computers and computer information (18 U.S.C. § 1030).

To educate federal prosecutors and agents on intellectual property rights, the General Litigation and Legal Advice Section first published a monograph on criminal copyright prosecutions in 1989. Significant changes in both law and technology have necessitated a new edition of the manual with an expanded focus on trafficking in counterfeit goods and a new section on the theft of trade secrets. We hope that this edition of the manual will be a useful resource -- at least until further changes in law and technology mandate yet another revision. In order for us to stay abreast of the current developments in this rapidly evolving area of the law, we would like to hear about prosecutions involving the criminal intellectual property statutes. Please call us at (202) 514-1026 to report such a prosecution. Finally, please also contact us with any comments, corrections or contributions regarding this manual¹ or for legal advice or litigation assistance.

The manual was written by Stevan D. Mitchell and Peter J.G. Toren with the assistance of David E. Green, under the supervision of Scott Charney, Chief, Computer Crime and Intellectual Property Section, and Martha Stansell-Gamm, Deputy Chief, Computer Crime and Intellectual Property Section.

¹ This text is not intended to create or confer any rights, privileges or benefits to prospective or actual witnesses or defendants. It is also not intended to have the force of law or of a United States Department of Justice directive. See United States v. Caceres, 440 U.S. 741 (1979).

TABLE OF CONTENTS

INTRODUCTION	i
I. THE PROTECTION OF INTELLECTUAL PROPERTY -- AN OVERVIEW	1
A. INTRODUCTION	1
B. COPYRIGHTS, TRADEMARKS, TRADE SECRETS, AND PATENTS	1
1. Copyrights	1
2. Trademarks	2
3. Trade Secrets	2
4. Patents	3
II. THE PROTECTION OF COPYRIGHTS	5
A. INTELLECTUAL PROPERTY ENTITLED TO COPYRIGHT PROTECTION	5
1. Historical Grounds for Copyright Protection	5
2. Requirements for Copyright Protection	7
a. <i>Originality</i>	7
b. <i>Fixed medium of expression</i>	8
c. <i>Registration and notice</i>	9
3. Nature of the Rights Protected by Copyrights	10
4. Limitations on Exclusive Rights	11
5. Computer software	12
III. CRIMINAL REMEDIES FOR COPYRIGHT VIOLATIONS	17
A. CRIMINAL COPYRIGHT INFRINGEMENT: 17 U.S.C. § 506(a) AND 18 U.S.C. § 2319	17
1. The Elements of Criminal Copyright Infringement	18
a. <i>Existence of a valid copyright</i>	19
b. <i>Infringement</i>	19
c. <i>Willfulness</i>	23
d. <i>Commercial advantage or private financial gain</i>	24
(1) Discrete monetary transactions	25
(2) Bartering	26
e. <i>The first sale doctrine in criminal cases</i>	27
(1) Proving absence of first sale	29
2. Drafting the Indictment	31

a.	<i>10 or More Copies</i>	31
b.	<i>Retail Value</i>	33
c.	<i>Equitable charging considerations</i>	33
3.	Other Possible Charges: Money Laundering and RICO	35
4.	Juvenile Prosecutions	36
5.	Penalties for Criminal Copyright Infringement	37
a.	<i>Statutory penalties</i>	37
b.	<i>Sentencing guidelines</i>	37
c.	<i>Other possible enhancements</i>	39
B.	TRAFFICKING IN SOUND RECORDINGS OF LIVE MUSICAL PERFORMANCES: 18 U.S.C. § 2319A	40
C.	OTHER TITLE 17 CRIMINAL PROVISIONS PROTECTING COPYRIGHTS	41
1.	Protection of Copyright Notices, 17 U.S.C. §§ 506(c) and (d)	41
2.	False Representations in Copyright Applications, 17 U.S.C. § 506(e)	42
D.	OTHER TITLE 18 OFFENSES	42
1.	Trafficking in Counterfeit Labels, 18 U.S.C. § 2318	42
2.	Interstate Transportation of Stolen Property, 18 U.S.C. § 2314	44
3.	Mail and Wire Fraud, 18 U.S.C. §§ 1341 and 1343	45
4.	Smuggling, 18 U.S.C. § 545	47
E.	STATUTE OF LIMITATIONS	47
F.	FORFEITURE	47
1.	Criminal Forfeiture	48
2.	Civil Forfeiture	48
G.	REPORTING REQUIREMENTS	49
H.	ALTERNATIVE STATE REMEDIES	50
IV.	PROTECTION OF TRADEMARKS	51
A.	INTELLECTUAL PROPERTY ENTITLED TO TRADEMARK PROTECTION	51
1.	Constitutional Limits on Trademark Protection	51
2.	Nature of the Rights Protected by Trademarks	52
3.	Statutory Limits on Trademark Protection	52
a.	<i>Distinctiveness</i>	53
b.	<i>Use in commerce</i>	54
4.	Limitations on Exclusive Rights	55

B.	THE CRIMINAL LAW	55
1.	Overview of Statute	55
2.	Elements	56
a.	<i>Trafficking in goods or services</i>	56
b.	<i>Trafficking was intentional</i>	56
c.	<i>The defendant used a "counterfeit mark"</i>	57
d.	<i>The defendant knew that the mark was counterfeit</i>	58
3.	Defenses	59
a.	<i>Lanham Act defenses</i>	59
b.	<i>Overrun or "grey market goods"</i>	59
4.	Charging Decisions	60
a.	<i>Intent of statute</i>	60
b.	<i>Money laundering/RICO</i>	61
c.	<i>Equitable charging considerations</i>	61
(1)	Extent of civil recovery	62
(2)	Violation of existing civil order--contempt	62
d.	<i>Monetary damages</i>	62
e.	<i>Units of prosecution</i>	63
f.	<i>Juvenile prosecutions</i>	63
C.	PENALTIES	64
1.	Statutory	64
2.	Sentencing Guidelines	64
3.	Forfeiture	66
a.	<i>Criminal</i>	66
b.	<i>Civil</i>	66
D.	CONTRASTING THE TRADEMARK AND THE COPYRIGHT ACT	67
E.	CHARGING BOTH CRIMINAL COPYRIGHT AND TRADEMARK VIOLATIONS	68
V.	PROSECUTION OF THEFT OF TRADE SECRETS	70
A.	INTRODUCTION	70
B.	THE ECONOMIC ESPIONAGE ACT OF 1996	71
1.	Overview of the Statute	71
2.	Elements common to §§ 1831 and 1832	72
a.	<i>Misappropriation</i>	73
b.	<i>Knowledge</i>	73
c.	<i>Trade secret</i>	74
3.	Additional § 1831 Element	77

a.	<i>Intent to benefit a foreign government</i>	77
4.	Additional section 1832 elements	79
a.	<i>Economic benefit to a third party</i>	79
b.	<i>Intent to injure the owner of the trade secret</i>	79
c.	<i>Interstate or foreign commerce</i>	79
5.	Defenses	80
a.	<i>Parallel development</i>	80
b.	<i>Reverse engineering</i>	80
c.	<i>General knowledge</i>	81
d.	<i>The First Amendment</i>	82
6.	Criminal Forfeiture	82
7.	Civil Proceedings	83
8.	Confidentiality	83
9.	Extraterritoriality	84
10.	Statutory Penalties	84
11.	Department of Justice Oversight	85
C.	OTHER POSSIBLE CHARGES	85
1.	Introduction	85
2.	18 U.S.C. § 2314	86
a.	<i>Elements</i>	86
(1)	Transportation in interstate commerce	87
(2)	Goods, wares and merchandise	87
(3)	Goods must have a value of \$5,000 or more	89
(4)	Stolen, converted or taken by fraud	90
b.	<i>Venue</i>	90
3.	18 U.S.C. § 2315	91
4.	18 U.S.C. §§ 1341 and 1343	91
5.	18 U.S.C. § 1905	93
6.	18 U.S.C. § 1030	94
7.	State Law	94

VI. APPENDICES A-1

Appendix A:	List of Contact Persons	A-1
Appendix B:	Sample Indictment - 18 U.S.C. § 2319 (Misdemeanor)	B-1
Appendix C:	Sample Indictment - 18 U.S.C. § 2319 (Felony)	C-1
Appendix D:	Sample Indictment - 18 U.S.C. § 2320	D-1
Appendix E:	Sample Indictment - 18 U.S.C. § 1831	E-1
Appendix F:	Sample Indictment - 18 U.S.C. § 1832	F-1
Appendix G:	Search Warrant Affidavit (Electronic Environment)	G-1
Appendix H:	Sample Language for Jury Instructions - 18 U.S.C. § 2319	H-1
Appendix I:	Sample Language for Jury Instructions - 18 U.S.C. § 2320	I-1
Appendix J:	Sample Language for Jury Instructions - 18 U.S.C. § 1831	J-1
Appendix K:	Sample Language for Jury Instructions - 18 U.S.C. § 1832	K-1

Appendix L:	List of States with "True Name and Address" Statutes	L-1
Appendix M:	State Criminal Trade Secret Statutes	M-1
Appendix N:	Legislative History - Copyright Felony Act	N-1
Appendix O:	Legislative History - Economic Espionage Act of 1996	O-1
Appendix P:	Table of Authorities	P-1

INTRODUCTION

The emergence of a truly global marketplace has created an increased demand for U.S. brand-named consumer goods and, unfortunately, a concomitant rise in illegal copying and reproduction of these goods. The illicit trade in counterfeit records, films, audio and videotapes, compact disks, computer programs and other goods has also been greatly facilitated by the ease with which such goods can be reproduced and distributed. American companies and businesses are losing vast sums of money as a result of this bootlegging, piracy, and counterfeiting.² In addition, in the most extreme cases, lives are being jeopardized through the unwitting use of inferior counterfeit products.

Information, itself, has also become increasingly valuable. With the end of the cold war, the focus of foreign espionage is no longer directed solely towards obtaining American military secrets, but to obtaining valuable proprietary information from U.S. companies. This theft of trade secrets has also been facilitated by emerging technology.

Investigations by federal law enforcement agencies must become more sophisticated. In the past, criminal investigations regarding intellectual property rights mainly targeted readily identifiable commercial operations. Law enforcement agents would purchase pirated material and then obtain search warrants for additional pirated or counterfeit materials available for sale to the public. Due to developing technology, however, this contraband can now be transferred electronically in a number of ways. Pirated computer programs, for example, can be copied and transferred over the Internet to hundreds of individuals in seconds, often making these electronic transfers difficult to detect and prosecute.

Similarly, a person stealing trade secrets no longer has to physically copy documents because much scientific and technical information is now stored on computers. Instead of copying hundreds of pages of information on a duplicating machine, a person can download that material onto a single computer disk,³ which can be easily concealed in a pocket. The information on the disk can then be sent or transmitted anywhere in the world without ever engendering the employer's suspicions. Additionally, if a thief is able to illegally penetrate a company's computer system, he or she can download that company's trade secrets and transmit them on international computer networks without removing the originals from the victim company.

² The terms "bootlegging," "piracy," and "counterfeiting" are similar but not synonymous. "Bootlegging" generally refers to the unauthorized recording and distribution of musical performances. "Piracy" involves the unauthorized reproduction of an existing copyrighted work or distribution of an infringing copy. However, the original packaging or graphics of the genuine merchandise are not copied. "Counterfeiting," by contrast, occurs when an infringer not only reproduces and distributes infringing merchandise, but also copies the genuine packaging of the product. In such cases, the counterfeiter is attempting to pass off his or her products as legitimate goods produced by the original manufacturer.

³ A 3.5 inch high-density computer disk can store approximately 720 pages of text.

By enacting felony provisions for, among other things, unauthorized reproduction or distribution of copyrighted works, trafficking in counterfeit trademarked goods, and theft of trade secrets, Congress has clearly evinced an intent to treat the misuse of intellectual property as a serious matter. This manual begins with an overview of the protection of intellectual property, and discusses the basic scope of copyright, trademark, trade secret, and patent law. It then focuses on criminal copyright infringement, describing specific statutes and demonstrating their application in criminal copyright prosecutions. Additional sections of the manual then address federal laws which prohibit trafficking in counterfeit goods. The last section discusses the prosecution of trade secret thefts and analyzes the Economic Espionage Act of 1996. Note all prosecutions under this Act must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. Finally, attached as appendices are a list of contact persons, model indictments, search warrant affidavits, jury instructions, a list of state criminal trade secret statutes, and the legislative histories of the Copyright Felony Act and the Economic Espionage Act of 1996.

I. THE PROTECTION OF INTELLECTUAL PROPERTY -- AN OVERVIEW

A. INTRODUCTION

The importance of the protection of intellectual property to the economic well-being and security of the United States cannot be overestimated. As one court put it, "[t]he future of the nation depends in no small part on the efficiency of industry, and the efficiency of industry depends in no small part on the protection of intellectual property." Rockwell Graphic Systems, Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991).

In many cases, civil remedies, including statutory damages, are adequate to compensate victims in copyright, trademark, trade secret, and patent cases. However, in an increasing number of cases, federal criminal prosecutions are warranted against flagrant infringers who might otherwise continue to flourish despite civil actions against them. These criminal investigations may also uncover evidence of related crimes, such as the unlawful importation of counterfeit goods. Additionally, since the theft of American trade secrets by foreign countries and companies is on a steep rise, only the federal government has the resources and reach to investigate and prosecute as needed. Further, federal criminal prosecutions often deter similar crimes throughout and across affected industries, and send a clear message to our international counterparts that protecting Intellectual Property Rights ("IPR") is a major concern of the United States.

B. COPYRIGHTS, TRADEMARKS, TRADE SECRETS, AND PATENTS

The protection of intellectual property can be divided into four general categories: (1) copyrights; (2) trademarks; (3) trade secrets; and (4) patents. Unlike the first three categories, patent infringement carries only civil remedies. Thus, this manual addresses violations in the first three areas. As an initial matter though, it is important to understand the basic scope each of these four areas of intellectual property.

1. Copyrights

The law of copyright, in general, protects "original works of authorship" including the following broad categories: literary works, musical works, dramatic works, pantomimes, pictorial, graphic, sculptural works, motion pictures, sound recordings, and architectural works. 17 U.S.C. § 102(a). It protects only a work's expression, not its underlying ideas; for example, one cannot copyright a machine process for manufacturing shoes. Copyright protection attaches when the

work is "fixed in a tangible medium of expression."⁴ Once in place, it extends to the embodiment of the work itself, protecting against unlicensed reproduction, distribution, display, performance, or modification of the copyrighted work. See 17 U.S.C. § 106. Remedies for infringement may include injunctive relief; monetary relief in the form of damages (lost profits), profits (gained by defendant in excess of lost profits) or statutory damages; impoundment and destruction of infringing material; criminal penalties; and attorney's fees and costs.

2. Trademarks

If copyright is the law of authorship, trademark is the law of consumer marketing and advertising. Trademarks are given federal protection by the Lanham Act. 15 U.S.C. § 1051 et seq. The Lanham Act, in general, prohibits the imitation and unauthorized use of a trademark which is defined as "any word, name, symbol or device or any combination [used by a person] to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown." 15 U.S.C. § 1127. If the trademark is used to identify the source of the goods as well as the goods themselves, it is known more specifically as a service mark. The purpose of a trademark is to signify a single source of product and a certain level of quality to all consumers. Thus, trademarks, unlike other forms of intellectual property, are always connected to some commercial activity or item and have no function or independent existence apart from such goods or services. To be granted trademark protection, an applicant must demonstrate that the mark is actually used, and has been continuously used, in commerce. Remedies for infringement may include injunctive relief; monetary relief in the form of damages (lost profits), profits (gained by defendant in excess of lost profits) or statutory damages (trebled when appropriate); seizure and destruction of infringing material; criminal penalties; and attorney's fees and costs.

3. Trade Secrets

In general, a trade secret is any formula, pattern, device or compilation of information used in a business to obtain an advantage over competitors who do not know or use it. Perhaps the most famous trade secret is the formula for manufacturing Coca-Cola. Coca-Cola was accorded trade secret protection in 1920 because the recipe had been continuously maintained as a trade secret since the company's founding in 1892, and it exists to this day. See Coca-Cola Bottling Co. v. Coca-Cola Co., 269 F. 796, 799 (3d Cir. 1920).

⁴ "A work is 'fixed' in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." 17 U.S.C. § 101.

Until recently, with one very minor exception,⁵ there was no specific federal law which criminalized the theft of trade secrets. Federal prosecutors were limited to using other laws, such as the Interstate Transportation of Stolen Property Act, 18 U.S.C. §§ 2314 and 2315, and the Mail and Wire Fraud statutes, 18 U.S.C. §§ 1341 and 1343, to prosecute individuals for the theft of trade secrets. However, in recognition of this enforcement gap and of the increasing importance of intellectual property to the economic well-being of the United States, Congress enacted The Economic Espionage Act of 1996 effective October 11, 1996. This Act creates two separate provisions which criminalize the theft of trade secrets. The first provision penalizes the theft of trade secrets when the theft is done to benefit a foreign government, instrumentality or agent.⁶ 18 U.S.C. § 1831. In contrast, the second provision makes criminal the more common commercial theft of trade secrets, regardless of who benefits. The Act also provides for criminal forfeiture and permits the use of civil proceedings by the United States to enjoin violations. Finally, it seeks to protect the confidentiality of trade secrets during litigation and provides for extraterritorial jurisdiction when the thief is an American citizen or a permanent resident of the United States. 18 U.S.C. §§ 1833-1837.

4. Patents

If copyright is the law of authorship and trademarks is the law of marketing, patents is the law of invention. A patent can be obtained for "any new and useful process, machine, manufacture, or composition of matter, or any new or useful improvement thereof" 35 U.S.C. § 101. A patent gives the patentee the right to exclude others from making, using, and selling devices that embody the claimed invention.⁷ See 35 U.S.C. § 271(a). In order to be awarded a patent by the Patent and Trademark Office, the subject matter must be both novel and a step beyond the prior art which, together, is known as "non-obviousness." See 35 U.S.C. § 103.

Patents protect products and processes, not pure ideas. For example, Albert Einstein could not have received a patent for his novel ideas on the theory of relativity. However, methods

⁵ 18 U.S.C. § 1905 provides, inter alia, misdemeanor sanctions for the unauthorized disclosure of government information, including trade secrets, by a government employee.

⁶ In general, the test of whether a foreign company can be prosecuted under 18 U.S.C. § 1831 is whether "the activities of the company are from a practical and substantive standpoint, foreign government directed." 142 Cong. Rec. S12201, S12201 (daily ed. Oct. 2, 1996). Of course, if this requirement cannot be met, the foreign company can still be prosecuted under 18 U.S.C. § 1832.

⁷ The popular notion that a patent grants the patentee the exclusive right to make, use, and sell his invention is erroneous. A patent gives you the right to exclude others from making, using or selling your invention. For example, if a chair with a seat and four legs is patented by inventor A, inventor B may obtain a patent for a chair with a seat, four legs and an armrest, but this patent does not allow him to make, use, or sell his chair because that would infringe A's patent for a chair with four legs and a seat.

for using this theory in a nuclear power plant are patentable. Unlike copyrights, patent rights do not vest until the patent is granted although, pending approval, the substance of many patent applications may be protected under trade secret laws. Since June 8, 1995, upon grant, patents last for a maximum of 14 or 20 years from filing depending on whether it is a design or a functional patent. Remedies for patent infringement include injunctive relief, damages (which may be trebled for willful violations), attorney's fees in exceptional cases, and costs.

There are no federal laws that criminalize patent infringement.⁸ This perhaps reflects the difficulty of proving that a person infringed a patent with the requisite mens rea for a criminal violation, given the possibility of independent creation and the arcane nature of the patent approval process conducted by the United States Patent Office. Kent Walker, Federal Criminal Remedies for the Theft of Intellectual Property, 16 Hastings Comm/Ent. L.J., 681, 686-87 (1994).

⁸ As of this writing, Congress has not provided criminal penalties for reproduction or distribution of goods that infringe patents. Congress has relied instead on affording plaintiffs a civil cause of action that makes treble damages and attorney's fees available for willful infringement. See 35 U.S.C. §§ 281-294. The only federal criminal statute currently dealing with patents makes it a felony to make, forge, counterfeit, or otherwise alter letters patent, or to pass or publish same knowing them to have been forged. 18 U.S.C. § 497.

Trade secret laws might be available in cases that otherwise closely resemble the misappropriation or wrongful use of patented concepts. It may take years, for example, for a patent application to be fully processed and for a patent to issue. In the intervening years, the information contained in a patent application may be entitled to trade secret protection under state laws or under the recently enacted Economic Espionage Act of 1996.

II. THE PROTECTION OF COPYRIGHTS

A. INTELLECTUAL PROPERTY ENTITLED TO COPYRIGHT PROTECTION

The substantive copyright laws are codified in Title 17 of the United States Code, which sets forth requirements and procedures for obtaining copyrights. Copyright protection only extends to certain types of property, defined by statute and subject to constitutional limitations. These constitutional and statutory constraints are discussed below.

1. Historical Grounds for Copyright Protection

The Constitution gives Congress the power to enact laws designed "[t]o Promote the Progress of Science and Useful Arts,⁹ by securing for Limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. CONST. art. I, § 8, cl. 8. The first Copyright Act that Congress passed under this power only protected "books," "maps" and "charts." See Act of May 31, 1790, ch. 15, 1 Stat. 124. The Supreme Court has since made it clear, however, that Congress' constitutional authority in the area extends well beyond written works to other media. As the Court has noted, this authority is not defined in a "narrow literal sense but, rather, with the reach necessary to reflect the broad scope of constitutional principles." Goldstein v. California, 412 U.S. 546, 561 (1973). Thus, the term "Author," in its constitutional sense, has been read to denote an "originator," or one "to whom anything owes its origin." Id. (quoting Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 58 (1884)). Similarly the word "writings" has been construed broadly "to include any physical rendering of the fruits of creative intellectual or aesthetic labor." Id. Thus, Congress' constitutional authority to establish copyrights reaches all tangible media of artistic expression, including photographs, motion pictures and sound recordings. See Goldstein, 412 U.S. at 562 n.17. Congress has exercised this authority, providing federal copyright protection to an increasingly broad range of intellectual properties. See Goldstein v. California, 412 U.S. 546, 562 n.17 (1973).

Congress initially relied upon civil sanctions to protect copyrights. Beginning in 1909, however, Congress also imposed criminal penalties for certain types of copyright infringement. See Act of March 4, 1909, ch. 28, 35 Stat. 1082. Adopting a "step-by-step, carefully considered

⁹ Under usage of the time, "Science" was the subject matter of copyright, "Useful Arts" the subject matter of patents.

approach," Congress has gradually expanded the role of federal law enforcement in this field. Dowling v. United States, 473 U.S. 207, 225 (1985).¹⁰

Prior to 1976, copyrights were protected in this country through a dual system. The federal government provided limited statutory rights for intellectual property, while state statutory and common laws established roughly equivalent protection for a range of intellectual properties. This dual system was, quite accurately, characterized as "anachronistic, uncertain, impractical, and highly complicated." H.R. Rep. No. 1476, 94th Cong., 2d Sess. 1, 130, reprinted in 1976 U.S. Code Cong. & Admin. News, 5659, 5745 (1976). Under this system, federal statutory copyright protection differed from common law copyrights, and state statutory and common law copyrights varied from jurisdiction to jurisdiction.

In 1976, Congress fundamentally changed this system by introducing a single preemptive federal statute. 17 U.S.C. § 301.¹¹ "Section 301 in effect establishes a two-pronged test to be applied in preemption cases." Crow v. Wainwright, 720 F.2d 1224, 1225 (11th Cir. 1983), cert. denied, 469 U.S. 819 (1984). See also Daboub v. Gibbons, 42 F.3d 285 (5th Cir. 1995); Rosciszewski v. Arete Associates, Inc., 1 F.3d 225 (4th Cir. 1993). Under this preemption test, the states are precluded from enforcing penalties for copyright violations if (1) the intellectual property at issue falls within the "subject matter of copyright" as defined by federal law and (2) the claimed property rights are "equivalent to" the exclusive rights provided by federal copyright law. Wainwright, 720 F.2d at 1225-26. The copyright act now precludes state criminal prosecutions for acts of copyright infringement. In all instances criminal prosecution for a copyright violation is possible only within the federal system.

In recent years, Congress has significantly broadened the scope of federal copyright protection. Federal law now protects artistic expression fixed on new types of media. For example, federal copyright protection now extends to sound recordings, computer software, and other forms of electronic data. See 17 U.S.C. §§ 102(a)(7), 117; see also Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1246-49 (3d Cir. 1983), cert. denied, 464 U.S. 1033 (1984). Video games are also now entitled to federal copyright protection. See Atari Games Corp. v. Oman, 888 F.2d 878 (D.C. Cir. 1989); United States v. O'Reilly, 794 F.2d 613, 614 (11th Cir. 1986) (citing Midway Mfg. Co. v. International Inc., 704 F.2d 1009 (7th Cir.)),

¹⁰ Prosecutors are advised to check the current status of 17 U.S.C. § 506 and 18 U.S.C. § 2319, the core criminal copyright statutes. At the time this manual was being prepared, Congress was considering several bills which would again amend the criminal copyright statute and its penalty provisions.

¹¹ The federal preemption provision, 17 U.S.C. § 301(a), provides that:

On and after January 1, 1978, all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by § 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by §§ 102 and 103, whether created before or after that date and whether published or unpublished, are governed exclusively by this title. Thereafter, no person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State.

cert. denied, 464 U.S. 823 (1983)); Williams Elecs, Inc. v. Arctic Int'l., Inc., 685 F.2d 870, 873-74 (3d Cir. 1982).

Finally, Congress has acted to significantly enhance criminal penalties. The penalties for criminal infringement of certain copyrights were increased dramatically in 1982, under 17 U.S.C. § 506 and 18 U.S.C. § 2319, and were extended in 1992 to cover all types of copyrighted works. Copyright infringement now may constitute a felony under federal law if at least ten infringing copies of any type of copyrighted work with a value of \$2,500 or more are made or distributed in a 180-day period. See 18 U.S.C. § 2319. Further, on September 13, 1994, Congress made a violation of 18 U.S.C. § 2319 a "specified unlawful activity" for the purposes of the money laundering statute, 18 U.S.C. § 1956, and on July 2, 1996, Congress amended 18 U.S.C. § 1961 to include copyright violations as predicate offenses under RICO.

2. Requirements for Copyright Protection

"As the text of the Constitution makes plain, it is Congress that has been assigned the task of defining the scope of the limited monopoly that should be granted to authors . . . in order to give the public appropriate access to their work product." Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984). Thus "the protection given to copyrights is wholly statutory," id. at 431 (citation omitted), while the remedies for copyright infringement remain confined to "only those prescribed by Congress." Thompson v. Hubbard, 131 U.S. 123, 151 (1889).

As of today, Congress has exercised this authority to provide copyright protection to all "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C. § 102(a). There are two primary components to this statutory definition. First, a work must be "original." In addition, that work must be "fixed in any tangible medium of expression." The requirements of originality and fixation set the outer limits of federal copyright protection. Finally, while copyright protection exists from the time of the creation of a work, see 17 U.S.C. §§ 101, 102(a), infringement actions may only be brought with respect to those works which have been registered with the Register of Copyrights. Therefore, this section also briefly explores copyright registration, and the (now optional) inclusion of the copyright notice on the work itself.

a. *Originality*

Originality is the "sine qua non" of copyright protection. Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340, 348 (1991). However, the standard for originality is minimal. The originality necessary to qualify for copyright protection calls for independent

creation, not novelty. As one court has stated, "[o]riginal in reference to a copyrighted work means that the particular work owes its origin to the author. No large measure of novelty is necessary." Alfred Bell & Co. v. Catalda Fine Arts, Inc., 191 F.2d 99, 103 (2d Cir. 1951). A work is not "original" if it is simply a copy of some other work existing in the public domain; however, for a work to be "original," an author needs only to contribute something more than a "merely trivial" variation -- something recognizably his or her own. See, e.g., Sid & Marty Krofft Television v. McDonald's Corp., 562 F.2d 1157, 1163 n.5 (9th Cir. 1977); L. Batlin & Son, Inc. v. Snyder, 536 F.2d 486, 490 (2d Cir.), cert. denied, 429 U.S. 857 (1976). Even the particular arrangement of otherwise non-copyrightable information may be copyrighted. See e.g., West Publishing Co. v. Mead Data Central, Inc., 799 F.2d 1219 (8th Cir. 1986) (upholding the district court's issuance of a preliminary injunction prohibiting Mead Data Central, the owner of LEXIS, from including Westlaw's "star pagination" keyed to West's case reports in the LEXIS system of computer-assisted legal research), cert. denied, 479 U.S. 1070 (1987); Kregos v. Associated Press, 937 F.2d 700, 706-07 (2d Cir.) (the selection of nine statistical categories for use on a baseball pitching form is copyrightable), cert. denied 510 U.S. 1112 (1994).

Note, however, that to qualify for protection the arrangement must be something out of the ordinary. The alphabetical listing of names in the white pages of a phone book, for instance, does not meet the requirement of originality. Feist Publications Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991). This originality requirement does not involve any assessment of the artistic quality of a work. An author's contribution may be copyrightable if it is in some way original, without regard to how poorly the artist's work may be viewed. See Gelles-Widmer Co. v. Milton Bradley Co., 313 F.2d 143, 146-47 (7th Cir.), cert. denied, 373 U.S. 913 (1963).

b. *Fixed medium of expression*

The fixation requirement of a copyright is defined by 17 U.S.C. § 101:

A work is "fixed" in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration. A work consisting of sounds, images, or both, that are being transmitted, is "fixed" for the purposes of this title if a fixation of the work is being made simultaneously with its transmission.

Within the broad parameters set by the originality and fixation requirements, all works of authorship are entitled to copyright protection. These works include, but are not limited to:

(1) literary works;¹² (2) musical works; (3) dramatic works; (4) pantomimes; (5) pictorial, graphic, and sculptural works;¹³ (6) motion pictures;¹⁴ (7) sound recordings;¹⁵ and (8) architectural works.¹⁶ 17 U.S.C. § 102(a).

c. *Registration and notice*

While an author's copyright is technically created at the moment a particular work is fixed, registration of a copyright is a prerequisite to any infringement action, civil or criminal. See 17 U.S.C. § 411(a); see also United States v. Backer, 134 F.2d 533, 535 (2d Cir. 1943). A work need not be registered prior to an act of infringement, but rather before a civil or criminal case is filed. However, to be entitled to recover statutory damages and attorney's fees in a civil case, the work must have been registered prior to commencement of the infringement for which such remedies are sought. See 17 U.S.C. § 412.

Registration requires only the completion of an application, a \$20 filing fee, see 17 U.S.C. § 708, and deposit of the work (or significant portions of the work) with the Library of Congress. See 17 U.S.C. § 408. While the process of registration normally takes several months, industry associations and representatives are often capable of assisting individual copyright holders in expediting the process in anticipation of litigation. A certificate of registration, if obtained within five years of the date of first publication, constitutes prima facie evidence of the validity of a copyright. 17 U.S.C. § 410(c).

¹² " 'Literary works' are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied." 17 U.S.C. § 101. Computer software is protected as a "literary work." See Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1246-49 (3d Cir. 1983); 17 U.S.C. § 117.

¹³ " 'Pictorial, graphic, and sculptural works' include two-dimensional and three-dimensional works of fine, graphic, and applied art, photographs, prints and art reproductions, maps, globes, charts, diagrams, models, and technical drawings, including architectural plans." 17 U.S.C. § 101.

¹⁴ " 'Motion pictures' are audiovisual works consisting of a series of related images which, when shown in succession, impart an impression of motion, together with accompanying sounds, if any." 17 U.S.C. § 101. Video games are often treated as audiovisual works. See Atari Games Corp. v. Oman, 888 F.2d 878 (D.C. Cir. 1989); United States v. O'Reilly, 794 F.2d 613, 614 (11th Cir. 1986) (collecting cases).

¹⁵ " 'Sound recordings' are works that result from the fixation of a series of musical, spoken, or other sounds, but not including the sounds accompanying a motion picture or other audiovisual work, regardless of the nature of the material objects, such as disks, tapes, or other phonorecords, in which they are embodied." 17 U.S.C. § 101.

¹⁶ "An 'architectural work' is the design of a building as embodied in any tangible medium of expression, including a building, architectural plans, or drawings. The work includes the overall form as well as the arrangement and composition of spaces and elements in the design, but does not include individual standard features." 17 U.S.C. § 101.

Publishing a notice of copyright on the work itself, while formerly a prerequisite for registration, is now optional for works published in the United States after March 1, 1989. Though optional, the copyright notice can be used as evidence of defendants' willfulness in criminal cases when the notice was displayed prominently on a work that has been infringed.

3 Nature of the Rights Protected by Copyrights

In addition to describing the works that are entitled to copyright protection, Congress has defined the exclusive rights that a copyright confers on the owner. Federal law grants the owner of a copyright the exclusive right to reproduce, distribute, and publicly display or perform the copyrighted work, as well as to prepare derivative works based upon the original copyrighted work. 17 U.S.C. § 106(1)-(5). "An unlicensed use of the copyright is not an infringement unless it conflicts with one of the[se] specific exclusive rights conferred by the copyright statute." Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 447 (1984) (citing Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 154-55 (1975)).¹⁷ Therefore, these five exclusive rights establish the universe of acts which may constitute copyright infringement.

The monopoly established by a copyright is limited in scope. A copyright is simply an exclusive right to a particular work, i.e., to the expression of some idea in a specific format. It does not confer any monopoly in or rights to the underlying ideas, concepts or principles embodied in that work. See 17 U.S.C. § 102(b) ("In no case does copyright protection . . . extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery . . .").¹⁸ Therefore, the rights of a copyright owner are infringed only by the copying or direct appropriation of a particular work, and not by the use of similar ideas or concepts in a different work.¹⁹ Similarity in expression is not infringing to the extent that the underlying idea dictates the manner in which it is expressed. In such cases ideas and expression are said to be

¹⁷ Twentieth Century has been superseded by statute on other grounds.

¹⁸ As a leading treatise on copyright law explains:

The policy rationale underlying the Act's exclusion of ideas from copyright protection is clear. To grant property status to a mere idea would permit withdrawing the idea from the stock of materials that would otherwise be open to other authors, thereby narrowing the field of thought open for development and exploitation. This effect, it is reasoned, would hinder rather than promote the professed purpose of the copyright laws, i.e., "the progress of science and useful arts."

3 MELVILLE NIMMER, DAVID NIMMER, Nimmer on Copyright § 13.03[B] at 13-69 to -70 (footnotes omitted).

¹⁹ This dichotomy between idea and expression can be illustrated by an example. A playwright, like William Shakespeare, could copyright a particular work, Romeo and Juliet. That copyright would protect the playwright from direct theft of his work. However, the copyright would not give Shakespeare the exclusive right to use the concept of star-crossed lovers in plays or to exclude others from writing a play based on that idea. See PAUL GOLDSTEIN, Copyright's Highway, The Law and Lore of Copyright from Gutenberg to the Celestial Jukebox, 205 (1994).

"merged" and copyright protection is unavailable in order to prevent the de facto monopoly over the idea. Kepner-Tregoe Inc. v. Leadership Software Inc., 12 F.3d 527, 533 (5th Cir.) cert.denied ___ U.S. ___, 115 S. Ct. 82 (1994); see also Merritt Forbes & Co. v. Newman Inv. Secs., Inc., 604 F. Supp. 943, 951 (S.D.N.Y. 1985) ("where an underlying idea may only be conveyed in a more or less stereotyped manner, duplication of that form of expression does not constitute infringement, even if there is word for word copying.") (citation omitted).

4. Limitations on Exclusive Rights

The exclusive rights conferred by 17 U.S.C. § 106 are subject to a series of statutory limitations. The first set of limitations is described in 17 U.S.C. § 107 through § 120. Essentially these sections provide that certain specific uses of a copyrighted work do not violate the copyright. For the most part, these narrow statutory exemptions do not present problems of proof in criminal cases. Indeed, only one of these exemptions has constituted a significant issue in criminal prosecutions. That exemption is the "first-sale doctrine." This doctrine, which is now codified at 17 U.S.C. § 109, is discussed in detail at "*The first sale doctrine in criminal cases*," infra p. 27.

The monopoly created by a copyright is limited in another respect. The Constitution authorizes Congress to enact legislation "securing for limited times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. CONST. art.1, § 8, cl.8 (emphasis added). Thus, Congress is explicitly prohibited from creating monopolies in perpetuity over intellectual property and legislation providing for such monopolies must be limited in duration.

Historically, the American copyright system set these limits by providing copyright protection for a fixed period beginning from the date of either publication or registration of the work. In 1976, however, Congress departed from this statutory scheme and adopted a system in which copyright protection began with the creation of the work and "endure[d] for a term consisting of the life of the author and fifty years after the author's death." 17 U.S.C. § 302(a). This rule now generally defines the duration of copyrights obtained on works created after January 1, 1978. In addition, Congress has provided special rules relating to works created prior to January 1, 1978, but not published or copyrighted until after that date, and to works copyrighted prior to January 1, 1978. See 17 U.S.C. §§ 303-04. Copyrights owned by corporations are accorded special treatment under the "works made for hire" provision of the Copyright Act. 17 U.S.C. § 101.²⁰ The employer or the corporation is considered the author of a work made for hire by an employee of the corporation. 17 U.S.C. § 201(b). See also Trenton v. Infinity Broadcasting Corp., 865 F. Supp. 1416, 1426 (C.D. Cal. 1994). Because the life of a

²⁰ 17 U.S.C. § 101 defines a "work made for hire" as "a work prepared by an employee within the scope of his or her employment."

corporate author cannot be fixed, the duration of a corporate copyright created on or after January 1, 1978, instead of a life plus fifty term, endures for a term of seventy-five years from the year of first publication of such work, or a term of one hundred years from the year of its creation, whichever expires first. See 17 U.S.C. § 302.

5. Computer software²¹

It is now clear, particularly since passage of the Computer Software Copyright Act of 1980,²² that computer software is entitled to copyright protection.²³ While computer programs

²¹ Prosecutors should be aware that investigating and prosecuting computer software cases is fundamentally different from cases based on the more traditional copyright schemes, like those involving the illegal copying and distribution of copyrighted motion pictures and sound recordings. Many of these differences arise from the fact that computer software is reproduced and distributed in a digital, as opposed to an analog, recording format. Digital information can be reproduced, stored, and transported in ways that are qualitatively different from the ways we are accustomed to reproducing, storing, and transporting analog technologies.

Analog technologies, such as those employed to create phonograph records, analog sound tapes, or videocassette tapes, operate by capturing electromagnetic patterns that represent (or are analogous to) the sounds or pictures themselves. Those patterns are then captured on some storage media capable of representing these rapidly changing patterns. For example, to produce a phonograph record, sounds are converted into the motion of an instrument that literally "carves" representations of those sounds into a master copy. Almost identical copies of the master are then reproduced, whereupon, on playback, the motion of the stylus is retranslated back into sounds for listening. One result of this method is that the recording is invariably an inferior reproduction of the original performance, and each successive copy of a copy is invariably slightly inferior to the copy from which it was made.

Recordings made through digital media, by contrast, depend on an intermediate translation process, whereby individual sights or sounds are interpreted into a string of binary characters -- "1's" and "0's" -- which are recorded not as constantly varying analog representations, but as successive binary characters. Thus, recording a digitally encoded signal is simply a matter of recording the successive strings of binary characters, the "1's" and "0's," in the same order in which they appeared in the original. As a result, recordings can be reliably and accurately accomplished by relatively inexpensive equipment. Additionally, duplication does not have to take place in anything approximating "real time," and so high quality copies can be produced in seconds.

Perhaps the most significant consequence is that, to one who receives a digitally encoded recording, there is no discernable degradation in quality from the original. That is, if the binary strings are faithfully reproduced in the copy, then the end product -- be it a computer program, sound recording, or motion picture -- will be identical in quality to the original. This fact carries consequences for those seeking to investigate and prosecute crimes involving digital technology. For one thing, it is no longer a relatively simple matter to determine, by reference to the recording itself, whether it is a copy or an original, or where it might fail along the duplication chain. It also follows that, unfortunately for the victim of pirating offenses, there is no natural end to the distribution chain: there is no point at which successive generations of digital duplicates will become qualitatively unacceptable to the consumer.

²² Pub. L. No. 96-517, § 10, 94 Stat. 3028 (1980) (codified at 17 U.S.C. §§ 101, 117).

²³ For an overview of some of the challenges of proof encountered in copyright litigation pertaining to computer
(continued...)

are generally treated as literary works for copyright purposes, Whelan Associates, Inc. v. Jaslow Dental Library, Inc., 797 F.2d 1222, 1234 (3d Cir. 1986), cert. denied, 479 U.S. 1031 (1987), in some cases they may qualify as audiovisual works. They almost certainly qualify as such in the form of video games. See Red Baron-Franklin Park v. Taito Corporation, 883 F.2d 275, 278 (4th Cir. 1989), cert. denied, 493 U.S. 1058 (1990). Computer software is copyrightable in both its source code²⁴ and object code²⁵ and without regard to whether it is used to facilitate human interaction or merely used to give operating instructions to computers. See Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1246-49 (3rd Cir. 1983), cert. denied, 464 U.S. 1033 (1984). It also can be copyrighted without regard to the medium in which it is fixed, whether on magnetic or optical media, or printed on paper, or embedded in a computer chip. Id. at 1249. Thus, criminal charges may arise not only from infringing copies on traditional magnetic storage media like disks and tapes, but also from illegal copies of computer code contained on computer "chips." See, e.g., United States v. Hayes, 800 F. Supp. 1575 (S.D. Ohio 1992) (copying code to blank chips), aff'd in part, vacated in part, 995 F.2d 1066 (6th Cir. 1993), appeal after remand, 16 F.3d 1222 (6th Cir. 1994); United States v. Hux, 940 F.2d 314, 319 (8th Cir. 1991) (court upheld defendant's conviction under § 506(a) for copying 205 bytes from a computer chip which contained 16,384 bytes). Even the temporary loading of an unlicensed copy of a copyrighted computer program in a computer's random access memory (RAM) has been held to constitute an infringing reproduction of copyrighted software. See, e.g., MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir.), cert. denied, 510 U.S. 1033 (1994); Advanced Computer Services v. MAI Systems Corp., 845 F. Supp. 356 (E.D. Va. 1994). Similarly, the law is likely to be applied to so-called "multi-media" works, which are similar to audiovisual creations.

Further, protections for digitally encoded works have become greater. The October 1992 revisions to the Copyright Act create a felony for some willful infringements of copyrighted software. See 17 U.S.C. § 506, 18 U.S.C. § 2319. For a detailed discussion of 18 U.S.C. § 2319, see "CRIMINAL COPYRIGHT INFRINGEMENT: 17 U.S.C. § 506(a) and 18 U.S.C. § 2319," *infra*, p. 17.

Software violations are by no means limited to "over the counter" sales of computer diskettes containing infringing products. Rather, owing to the efficient manner in which computer

(...continued)

software, see Ronald L. Johnston, Toward an Effective Strategy in Software Copyright Litigation, 19 Rutgers Comp. & Tech. L.J. 91 (1993). Particularly useful to criminal prosecutors and investigators are the author's discussions of detecting and proving infringement, id. at 103, and evidence of copying, id. at 107.

²⁴ Source code is the original symbolic coding which programmers use to write computer programs. It is comprehensible to humans, but not to the computer that must execute it. Someone who steals source code can see how the program works and cannot only duplicate the program, but can modify it. The source code for a program can be also an extremely valuable trade secret.

²⁵ Object code (also called executable code) is the form to which source code must be converted for it to be executed by a computer. It is comprehensible to computers but not to most humans. This is the form in which computer programs are sold or licensed to the public.

software can be reproduced, stored and transferred, investigators can expect to encounter a full range of violations that make varied use of these characteristics from private, individual infringements to complex, commercial criminal operations.²⁶ For example, pirate copies need not be distributed "over the counter," but may change hands electronically through e-mail, electronic bulletin board systems or over the Internet. Infringing copies might also be distributed through "rental" schemes, in which legitimately purchased copies may be rented, for short periods of time, with the understanding that the software is to be copied and returned.²⁷

In some instances, copyright violations may occur in conjunction with otherwise legitimate sales or business transactions. Some computer hardware dealers may engage in a deceptive form of copyright infringement called "hard disk loading," i.e., loading unauthorized copies of software onto computers they sell as a way to cut costs and as an incentive for purchasers to buy the computers.

Some violations may be more complex, such as those involving Original Equipment Manufacturers (OEMs). An OEM is a hardware manufacturer that buys assorted computer components and builds complete systems. Many OEMs have licenses with the major software vendors which allow them to sell their computer systems along with a specified number of licensed programs. The OEMs, however, are not permitted to sell the software without the hardware, known as a "standalone" version. Copyright problems may arise, however, if an OEM were to willfully exceed the number of copies authorized by their agreement with the copyright holder or if the OEM sells standalone versions of the software. These circumstances, with the exception of rental arrangements falling within the scope of 17 U.S.C. § 109(b)(1)(A), may constitute criminal violations of the copyright act.²⁸

²⁶ Another consequence of digital recording technology is that a binary string of 1's and 0's can be stored --and hence concealed -- in any number of electronic devices. More and more household devices are being built to provide electronic storage capabilities, such as computer, telephone, and television components. Digital storage technology, coupled with digital communications technology, make off-site storage of information not only a possibility, but a reality that must be accounted for in investigations. It may no longer be sufficient, in some investigations, to conduct a search of a suspect's home or workplace. It may also be necessary to gather information from remote computers to which a suspect is known to have access. See Federal Guidelines to Searching and Seizing Computers, Department of Justice, Computer Crime and Intellectual Property Section, July 1994.

²⁷ Rental schemes, while often resulting in the proliferation of infringing copies for a commercial purpose, are nonetheless outside the reach of existing criminal statutes. See Computer Software Rental Amendments Act of 1990, 17 U.S.C. § 109(b)(1)(A) (prohibiting the unauthorized rental, lease or lending of legitimately purchased copies of a phonorecord or computer program); and § 109(b)(4) (declaring that violations of § 109(b)(1) "shall not be a criminal offense under section 506 or cause such person to be subject to the criminal penalties set forth in section 2319 of title 18.").

²⁸ In contrast to the federal anti-counterfeiting statute, 18 U.S.C. § 2320, the federal criminal copyright scheme contains no exemption for "overrun" goods, that is, goods produced by a licensed manufacturer but produced in amounts exceeding the scope of the license. Thus, willful violations of contractual conditions may deserve consideration under the criminal copyright laws. Prosecutors, in such instances, should carefully scrutinize whether the infringing copies

(continued...)

Many instances of software copyright infringement are difficult to detect and trace, as they may never involve the public sale or trading of infringing products. Rather, business entities or groups might make multiple pirate copies of software solely for their own internal use. Such internal use may still fall well within the reach of the applicable criminal provisions, which extend to those who, as will be discussed in more detail later, "infringe[] a copyright willfully and for purposes of commercial advantage or private financial gain." 17 U.S.C § 506(a). An entity that purchases a single-use copy of a popular software application, and then copies and uses that program on more than one workstation, not only commits copyright infringement, but also benefits economically from its savings by not having to purchase individual copies or a more expensive site license of the same computer program. If the program is used by employees on behalf of the business, the company would be hard-pressed to argue that its infringement was not "for purposes of commercial advantage or private financial gain." 17 U.S.C. § 506(a).

Similarly, reproducing and distributing copyrighted materials electronically may also give rise to criminal infringement charges. This is true whether copies of infringing software are reproduced for transmission by direct modem-to-modem file transfer, through the use of electronic mail (e-mail), through the use of a computer bulletin board system (BBS), or are transmitted over the Internet.

We caution, however, that the underlying civil laws defining "infringement" in an electronic environment have not yet been fully developed. Substantial doubt exists, for example, as to whether the mere electronic transmission of copyrighted works actually infringes a copyright owner's right of "distribution" which by the terms of 17 U.S.C. § 106(3) is limited to the "sale or other transfer of ownership, or by rental, lease, or lending." There is little doubt, however, that the electronic reproduction of copyrighted works in preparation for transmission clearly violates a copyright holder's well-settled rights. Therefore, absent the passage of a legislative amendment that would make "transmission" a protected act, we encourage investigators and prosecutors to treat cases that arise through the electronic transmission of copyrighted works as violations of the copyright holder's rights of reproduction, to present the evidence along these lines, and to charge these cases accordingly.

The majority of criminal copyright cases that implicate the use of computers and advanced technology will, for at least the next few years, probably focus on software rather than other digital works. But, as mentioned, the very same methods by which pirated software is reproduced and transmitted today are also being increasingly used to transmit most other forms of copyrighted works, including sound recordings, motion pictures, photographs, textual works, and even multi-media creations. Thus, the same techniques that are being developed for use against

(...continued)

might have been produced as a result of an honest error, such as a disagreement arising from unclear licensing terms, in which case the infringement would not be "willful." See "The Elements of Criminal Copyright Infringement," *infra*, p. 18.

software pirates will become applicable to those other types of copyright cases arising in an electronic environment.

III. CRIMINAL REMEDIES FOR COPYRIGHT VIOLATIONS

As previously noted, the criminal law now assumes greater significance in the protection of copyrights. This development is, in part, a consequence of the burgeoning trade in unlawfully reproduced records, tapes, films, and computer software. It is also a direct result of the increased attention paid to copyright issues by Congress and by federal law enforcement authorities.

The federal copyright statute, contained in Title 17 of the United States Code, provides for several separate criminal sanctions. At the outset, 17 U.S.C. § 506(a) imposes criminal penalties on certain acts of copyright infringement, and carries the most severe penalties of any Title 17 offense. Section 506(a) makes reference to 18 U.S.C. § 2319, which contains specific penalties and additional criminal elements. Section 506 also provides lesser criminal sanctions for conduct which does not constitute copyright infringement but which nonetheless undermines the integrity of the copyright system. See 17 U.S.C. § 506(c)-(e). Further, in 1994, Congress created 18 U.S.C. § 2319A, which expressly covers the unauthorized fixation of and trafficking in sound recordings and musical videos of live musical performances. Pub. L. No. 103-465, Title V, § 513(a), 108 Stat. 4974 (1994). These criminal provisions are discussed in seriatim.

A. CRIMINAL COPYRIGHT INFRINGEMENT: 17 U.S.C. § 506(a) AND 18 U.S.C. § 2319

The principal criminal statute protecting copyrighted works is 17 U.S.C. § 506(a). In 1982, special provisions for motion pictures and sound recordings were added to provide felony penalties for first-time offenders. While the criminal prohibition remained enumerated at 17 U.S.C. § 506(a), the felony penalties for unlawfully reproducing or distributing motion pictures or sound recordings were placed in § 2319 of Title 18. Individuals convicted for the first time of large-scale infringement²⁹ involving sound recordings or audiovisual works were subjected to a maximum penalty of up to five years' imprisonment, a \$250,000 fine, or both.

In 1992, Congress again amended § 2319. Pub. L. No. 102-561, 106 Stat. 4233 (1992). This section, as amended, now provides in part:

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsection (b) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

²⁹ The 1982 statute had made it a felony to reproduce or distribute, during any 180-day period, (1) at least 1000 phonorecords or copies infringing the copyright in one or more sound recordings or (2) at least 65 copies infringing the copyright in one or more motion pictures or other audiovisual works.

(b) Any person who commits an offense under subsection (a) of this section --

(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, with a retail value of more than \$2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

These new penalties make 17 U.S.C. § 506(a), which incorporates 18 U.S.C. § 2319 by reference, an effective criminal deterrent against the infringement of copyrights.³⁰

The 1992 amendments have made it possible to pursue felony sanctions for infringements of all types of copyrighted works, including computer software and copyrighted digitally encoded works.³¹ Felony penalties, however, only attach to violations involving reproduction or distribution in the quantity stated. It is a misdemeanor violation if the numerical and monetary thresholds are not met, or if the defendant is involved in the infringement of the right to prepare derivative works, or the right to publicly display or perform a copyrighted work.

1. The Elements of Criminal Copyright Infringement

There are four essential elements to a charge of criminal copyright infringement. In order to obtain a conviction under § 506(a), the government must demonstrate:

(1) that a valid copyright exists;

³⁰ Note that 18 U.S.C. § 3571 increases potential penalties for certain categories of offenders; therefore, it is necessary to consult both §§ 2319 and 3571 in order to ascertain the maximum fine.

³¹ When amending the penalty provisions relating to criminal copyright infringement, Congress eliminated distinctions between types of copyrighted works, some of which, such as phonorecords and motion picture films, had been afforded higher protections. Now, copyrighted computer software and other forms of electronic intellectual property are protected to the same extent as records and motion picture films. These amendments also made criminal provisions more generally applicable to smaller commercial operations by lowering the felony threshold level to 10 copies valued at more than \$2,500. See Pub. L. No. 102-561, 106 Stat. 4233 (1992).

- (2) that it was infringed by the defendant;
- (3) willfully; and
- (4) for purposes of commercial advantage or private financial gain.³²

See, e.g., United States v. Manzer, 69 F.3d 222, 227 (8th Cir. 1995) (infringement of computer program used in satellite descrambler modules); United States v. Hux, 940 F.2d 314, 319 (8th Cir. 1991); United States v. Wise, 550 F.2d 1180 (9th Cir.), cert. denied 434 U.S. 929 (1977). Conspiracies to violate the Act can be prosecuted under 18 U.S.C. § 371.

a. *Existence of a valid copyright*

The initial element of a criminal prosecution under 17 U.S.C. § 506(a) is that the victim has a valid copyright, which may be established by demonstrating that the formal requisites of copyright registration have been satisfied. In many instances, registration of a copyright can be proven simply by obtaining a certificate of registration from the Register of Copyrights. By law, a certificate of registration "made before or within five years after the first publication of the work shall constitute prima facie evidence of the validity of the copyright. . . ." 17 U.S.C. § 410(c); see also United States v. Taxe, 540 F.2d 961, 966 (9th Cir.) (in criminal case, certificate of registration provided prima facie proof of date of fixation), cert. denied, 429 U.S. 1040 (1976). Where a copyright registration certificate is produced, the burden shifts to the defendant to present evidence of copyright invalidity, existence of a license, or a defense to the infringement. See e.g., Autoskill Inc. v. National Educational Support Systems, Inc., 994 F.2d 1476, 1487 (10th Cir.), cert. denied, 510 U.S. 916 (1994). If the defendant contests the validity of a copyright, the prosecutor must make an independent evidentiary showing that a copyright is valid. This would involve showing that the copyright was not obtained by fraud and the registration certificate is genuine.

b. *Infringement*

Once the validity of the copyright is established, the government must then prove that the defendant "infringed" that copyright. Although the term "infringement" is not defined, *per se*, in the copyright statute, 17 U.S.C. § 501(a) provides that: "[a]nyone who violates any of the exclusive rights of the copyright owner as provided by [17 U.S.C. §§ 106 to 120] . . . is an

³² A minority of courts also require that the government prove the absence of a first sale, and thus some cases refer to this as a fifth element. However, the majority position is that the defendant must raise the first sale as an affirmative defense, and that the lack of a first sale need not be alleged in the indictment. The doctrine, the uncertainty surrounding its use, and its role in criminal copyright prosecutions are discussed separately at "*The first sale doctrine in criminal cases*," *infra* p. 27.

infringer of the copyright." Thus, the concept of infringement is defined by reference to the exclusive rights conferred on a copyright owner by 17 U.S.C. § 106. Those exclusive rights include the right to prepare derivative works, or to display or perform the work publicly, 17 U.S.C. § 106(4)-(5), along with the right to reproduce and distribute copies of the work, 17 U.S.C. § 106(1) & (3). Therefore, any unauthorized exercise of these rights will constitute an act of infringement and will give rise at least to a civil infringement claim by the copyright holder.

Note, however, that the felony provisions of 18 U.S.C. § 2319 apply only when the offense "consists of the reproduction or distribution, during any 180-day period, of at least 10 copies³³ or phonorecords, of 1 or more copyrighted works,³⁴ with a retail value of more than \$2,500."³⁵ 18 U.S.C. § 2319(b)(1) (emphasis and footnotes added). Infringement of rights other

³³ "Copies" are defined as:

material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. The term 'copies' includes the material object, other than a phonorecord, in which the work is first fixed. 17 U.S.C. § 101.

Requiring a minimum of 10 copies was intended to exclude from felony prosecution "children making copies for friends as well as other incidental copying of copyrighted works having a relatively low retail value." H.R. Rep. No. 997, 102 Cong., 2d Sess., at 6 (Oct. 3, 1992), reprinted in 1992 U.S. Code Cong. & Admin. News 3569, 3574 (1992).

³⁴ The Committee also noted:

The phrase "of one or more copyrighted works" is intended to permit aggregation of different works of authorship to meet the required number of copies and retail value. For example, a defendant's reproduction of 5 copies of a copyrighted word processing computer program having a retail value of \$1,300 and the reproduction of 5 copies of a copyrighted spreadsheet computer program also having a retail value of \$1,300 would satisfy the requirement of reproducing 10 copies having a retail value of at least \$2,500, if done within a 180 day period.

Id. at 6, U.S. Code Cong. & Admin. News at 3574.

³⁵ The drafting Committee left the term "retail value" "deliberately undefined, since in most cases it will represent the price at which the work is sold through normal retail channels." H.R. Rep. No. 997, 102 Cong., 2d Sess., at 6 (Oct. 3, 1992), reprinted in 1992 U.S. Code Cong. & Admin. News 3569, 3574 (1992).

The Committee acknowledged, however, that copyrighted works can be infringed before a retail value has been established -- such as is the case with software "beta-test" versions. (Beta test copies of software are those still under development that have not yet been sold to the public. They are circulated to select users for testing and evaluation. At the time they are circulated, however, the copyright holder may not have established the eventual retail price.) The Committee left it to the court, in such cases, to look to the "suggested retail price, the wholesale price, the replacement cost of the item, or financial injury caused to the copyright owner." Id. at 7, 1992 U.S. Code Cong. & Admin. News at 3575. In any case, it seems clear that the term "retail value" in this provision was intended to refer to the retail value of the infringed item, i.e., the legitimate item that was infringed. This seems to be true even though it appears to conflict with the approach taken under the Sentencing Guidelines, which look, for sentencing purposes, to the value of the

(continued...)

than the right of reproduction or distribution (such as infringement of public performance rights or the production of derivative works) remains a misdemeanor. Similarly, if the government fails to prove that the offense involved the requisite number of infringing copies (10 or more), reproduced or distributed within the requisite period (180 days), or did not meet the requisite retail value (more than \$2,500), the offense will be treated as a misdemeanor. See 18 U.S.C. § 2319(b)(3).

In cases alleging felony violations, proof of infringement typically involves evidence that the defendant produced or sold unauthorized copies of one or more works. Note that infringement can exist even when the defendant has not "stolen" the original work -- indeed, even when he bought a legal copy from which he has made the illegal ones. The copyright owner need not be deprived of possession of, or use of, his or her work in order for infringement to occur. Rather, the copyright laws protect an individual's rights in a creative work, which may include the right to distribute, or not distribute, as the owner pleases.

Generally, infringement is established by direct evidence of copying. Sid & Marty Krofft Television v. McDonald's Corp., 562 F.2d 1157, 1162 (9th Cir. 1977). However, since the actual copying of the copyrighted work is not often provable, circumstantial evidence may be used to prove that (1) the defendant had access to the copyrighted work and (2) that defendant's work is substantially similar to the copyrighted material. Computer Associates Intern., Inc. v. Altai, Inc., 982 F.2d 693, 701 (2d Cir. 1992); See also Kamar Intern. Inc. v. Russ Berrie & Co., 657 F.2d 1059 (9th Cir. 1981).

It is unnecessary to demonstrate that an allegedly infringing article is identical to the original work in all respects. See United States v. O'Reilly, 794 F.2d 613, 615 (11th Cir. 1986). Instead, infringement may be shown by simply demonstrating a "substantial similarity" between the original work and the suspect copy. See, e.g., Hoehling v. Universal City Studios, Inc., 618 F.2d 972, 977 (2d Cir.), cert. denied, 449 U.S. 841 (1980); McCulloch v. Albert E. Price, Inc., 823 F.2d 316 (9th Cir. 1987). A copy has been held to be "substantially similar" to an original work where "the [copy] is so similar to the [original] work that an ordinary reasonable person would conclude that the defendant unlawfully appropriated the [copyright owner's] protectible expression by taking material of substance and value." Atari, Inc. v. North American Philips Consumer Elec. Corp., 672 F.2d 607, 614 (7th Cir.) (citation omitted), cert. denied, 459 U.S. 880 (1982). This standard focuses on the similarities between the two works, rather than on any differences that may exist between them. Thus, "it is enough that substantial parts [of a copyrighted work] were lifted; no plagiarist can excuse the wrong by showing how much of his work he did not pirate." O'Reilly, 794 F.2d at 615 (quoting Sheldon v. Metro-Goldwin Pictures Corp., 81 F.2d 49, 56 (2d Cir.), cert. denied, 298 U.S. 669 (1936)). It should be emphasized that a finding of substantial similarity between a copyrighted work and an alleged infringing work

(...continued)

infringing items. See "Sentencing Guidelines," infra p. 37.

requires more than evidence of adherence to the general ideas expressed, because ideas in and of themselves cannot be copyrighted. See 17 U.S.C. § 102(b). ("In no case does copyright protection . . . extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery. . .").

In practice, this substantial similarity is generally demonstrated through a side-by-side comparison of the suspect copy with an authentic original. In several instances, defendants have argued that the government must compare these allegedly infringing copies against the originals maintained on file at the Registry of Copyrights in order to satisfy its burden of proof on this issue. See O'Reilly, 794 F.2d 613 (11th Cir. 1986); United States v. Shabazz, 724 F.2d 1536, 1539 (11th Cir. 1984). While some courts have agreed "that it is 'better practice' for the government to compare the counterfeit material with the duplicate registered with the copyright office," O'Reilly, 794 F.2d at 615, no court has accepted this defense argument. Thus, any authentic duplicate of the original may be used for the purpose of making this comparison.

In cases of copyright violations involving computer programs, it must also be determined whether or not existing copies were lawfully made pursuant to the provisions of 17 U.S.C. § 117.³⁶ If so, there has been no infringement.

Finally, the concept of infringement includes a host of statutory exceptions to the exclusive rights created by copyright. For the most part, these statutory exceptions do not create problems of proof in criminal cases. In fact, many of these limitations involve conduct which is already specifically exempted from criminal liability by the heightened proof requirements of 17 U.S.C. § 506(a) and 18 U.S.C. § 2319. For example, 17 U.S.C. §§ 110 and 118, which concern non-profit performances and displays of a copyrighted work, do not affect criminal prosecutions, since such prosecutions are limited to acts of infringement undertaken "for purposes of commercial advantage or private financial gain." See 17 U.S.C. § 506(a).

³⁶ 17 U.S.C. § 117 states:

Notwithstanding the provisions of section 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:

- (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or
- (2) that such new copy or adaptation is for archival purposes only, and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.

Any exact copies prepared in accordance with the provisions of this section may be leased, sold, or otherwise transferred, along with the copy from which such copies were prepared, only as part of the lease, sale, or other transfer of all rights in the program. Adaptations so prepared may be transferred only with the authorization of the copyright owner.

Other limitations, while theoretically applicable in criminal cases, have little practical impact on the government's burden of proof. For example, the equitable "fair use" doctrine, codified at 17 U.S.C. § 107, limits the exclusive rights of a copyright owner.³⁷ While serious questions of fair use may and often do arise in civil copyright infringement cases, as a practical matter, the fair use doctrine should not impose any additional burden on the government in a criminal infringement action. The prosecution is already required by 17 U.S.C. § 506(a) to demonstrate willful infringement conducted for purposes of commercial advantage or private financial gain. Proof of these elements, if sufficient, would virtually preclude any defense of non-infringing fair use.³⁸

c. *Willfulness*

To establish criminal intent, the government must prove that the defendant willfully infringed the copyright. See 17 U.S.C. § 506(a). The Supreme Court has recognized that the meaning of the word "willful" in criminal statutes has many meanings and "its construction is often . . . influenced by its context." Ratzlaf v. United States, 510 U.S. 135, 114 S. Ct. 655, 659 (1994)

³⁷ This section provides in full as follows:

Notwithstanding the provisions of sections 106 and 106A [exclusive rights in copyrighted works], the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include-

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of the above factors.

³⁸ Throughout progressive revisions to the criminal copyright laws, Congress has been careful to emphasize that the heightened mens rea element "serves to leave outside the reach of the criminal law losing parties in ordinary business disputes such as those involving reverse engineering of computer programs or contract disputes over the scope of licenses. . . . In cases where civil liability is unclear -- whether because the law is unsettled, or because a legitimate business dispute exists -- the Committee does not intend to establish criminal liability." H.R. Rep. No. 997, 102 Cong, 2d Sess., at 5, reprinted in 6 U.S. Code Cong. & Admin. News 3569, 3573 (1992).

(quoting Spies v. United States, 317 U.S. 492, 497 (1943)). Courts are in general agreement that in the copyright context a willful act must be "an act intentionally done in violation of the law." United States v. Wise, 550 F.2d 1180, 1194 (9th Cir.), cert. denied, 434 U.S. 929 (1977). Willful infringement also implies that "the act was committed by a defendant voluntarily, with knowledge that it was prohibited by law, and with the purpose of violating the law, and not by mistake, accident or in good faith." United States v. Cross, 816 F.2d 297, 300 (7th Cir. 1987); see also United States v. Manzer, 69 F.3d 222, 227 (8th Cir. 1995) (evidence that the copyrighted material bore a copyright notice was sufficient to put defendant on notice and "refute a defense based on innocent infringement").

But when defining willfulness, courts have differed in their interpretation of which of the two acts -- copying or infringing -- requires willful intent. The minority view, endorsed by the Second and Ninth Circuits, holds that "willful" means only intent to copy, not intent to infringe. See United States v. Backer, 134 F.2d 533, 535 (2d Cir. 1943) ("The [defendant] deliberately had the copies made . . ."); United States v. Taxe, 380 F. Supp. 1010 (C.D. Cal. 1974), aff'd in part and vacated in part, 540 F.2d 961 (9th Cir. 1976), cert. denied, 429 U.S. 1040 (1977). Or, put another way, there is no defense for mistake of law.

The majority view, however, requires intent to infringe (rather than intent to copy), and the government must demonstrate a "voluntary, intentional violation of a known legal duty." United States v. Moran, 757 F. Supp. 1046, 1049 (D. Neb. 1991) (defendant successfully persuaded finder of fact that he believed his practice of "insuring" legitimately owned copyrighted works by producing one and only one additional copy was permitted by copyright law). This construction, then, provides a significant exception to the maxim that "ignorance of the law is no excuse." Indeed, under this construction, if a trier of fact was satisfied that a defendant was not aware of the laws prohibiting copyright infringement, or was satisfied that the defendant did not believe his acts infringed, it might constitute a defense to the criminal charge. It would not, however, constitute a defense to civil infringement, as civil infringement remains a strict liability tort. It is thus crucial, in criminal cases, to amass evidence of intent in order to anticipate and rebut this "lack of intent" defense.

d. *Commercial advantage or private financial gain*

Beyond demonstrating willfulness, the government must prove that the defendant engaged in an act of infringement "for purposes of commercial advantage or private financial gain." See 17 U.S.C. § 506(a). Here the emphasis should be placed on "purposes," for it is irrelevant whether any profit was, in fact, realized. See United States v. Taxe, 380 F. Supp. 1010, 1018 (C.D. Cal. 1974), aff'd in part and vacated in part, 540 F.2d 961 (9th Cir. 1976), cert. denied, 429 U.S. 1040 (1977). All that is required is that the defendant engage in the infringing conduct with the hope or expectation of profit. See, e.g., United States v. Cross, 816 F.2d 297, 301 (7th Cir. 1987); United States v. Shabazz, 724 F.2d 1536, 1540 (11th Cir. 1984);

United States v. Wise, 550 F.2d 1180, 1195 (9th Cir.), cert. denied, 434 U.S. 929 (1977). The drafting committee's long-held purpose in retaining this requirement has been to exclude from criminal liability those individuals who willfully infringe copyrights solely for their own personal use. H.R.Rep. No. 997, 102 Cong., 2d Sess. at 5 (1992), reprinted in 1992 U.S. Code Cong. & Admin. News 3569, 3573 (1992).

In some cases courts have found the requisite commercial or financial purpose to be implicit in the conduct of the parties. See United States v. Cross, 816 F.2d 297, 301 (7th Cir. 1987) ("[W]e find that the presence of these seventeen second-generation videocassettes on [subject's] business premises may rationally give rise to the inference that they were maintained for commercial advantage or private financial gain."). Similarly, the court stated in United States v. Shabazz:

An employee identified specific tapes made in bulk under appellant's direction as reproduced for local and out of state sale. The appellant sold pirate tapes, solicited wholesale customers, and shipped large quantities of tapes out of state. This evidence is sufficient to show that the tapes produced were made with the intention to make a profit. It is not necessary that he actually made a profit. The only requirement is that he engaged in business 'to hopefully or possibly make a profit.'

724 F.2d 1536, 1540 (11th Cir. 1984) (citing United States v. Wise, 550 F.2d 1180, 1195 (9th Cir. 1977), cert. denied, 434 U.S. 929 (1977)); United States v. Moore, 604 F.2d 1228 (9th Cir. 1979).

Two different methods of showing profit are often relevant in copyright cases: discrete monetary transactions and bartering.

(1) Discrete monetary transactions

Evidence of discrete monetary transactions (i.e., the selling of infringing works for a particular price) provides, of course, the best evidence of financial gain. Nonetheless, it is not necessary to present such direct evidence; indeed, such a stringent requirement would ignore the plain wording of the statute, which requires only the showing of commercial or financial purpose. Thus, for example, in a computer bulletin board context, the requisite commercial purpose may be established by showing that the offenders displayed an intent to use software "libraries" they have assembled to attract subscribers to their bulletin board, who are then required to pay a fee for the privilege of accessing the copyrighted material.³⁹ Another example would be a computer store or

³⁹ Even boards that do not overtly advertise a particular fee for access may advertise and collect fees covertly, or
(continued...)

an original equipment manufacturer ("OEM," see "Computer Software," *supra* p. 12) that bundles or includes infringing software with computer hardware, and thus undercuts its competitors who include licensed copies of software in the price of a complete computer system.

(2) Bartering

A similar rationale should support the appropriate prosecution of so-called "bartering" cases. In bartering schemes, people trade infringing copies for other infringing items on either a one-for-one exchange or through the use of credit or "points" systems. It is a common misconception that if infringers fail to charge subscribers a monetary fee for infringing copies, they cannot be held to have engaged in criminal copyright infringement. Prosecutors should argue that the term "for purposes of commercial advantage or private financial gain" does not require the payment in money for the infringing merchandise, but includes payment by trading anything of value. Further, "it is irrelevant whether there was an exchange for value so long as there existed the hope" of some gain. United States v. Moore, 604 F.2d 1228, 1235 (9th Cir. 1979). Thus, when "bartering" results in the unauthorized dissemination of substantial amounts of infringing product without recompense to the copyright holders, vigorous prosecution is fully consistent with the purposes of the criminal copyright statute.⁴⁰

Further, several civil cases lend support for the criminal prosecution of "bartering" schemes that are run through computer bulletin board systems. In Sega Enterprises, Ltd. v. Maphia, 1996 WL 734409 (N.D. Cal., Dec. 18, 1996), the plaintiff accused the defendant, an owner and operator of a bulletin board system, of distributing the plaintiff's copyrighted computer programs. The district court granted plaintiff's motion for summary judgment for copyright infringement. The court first reasoned that the defendant did not directly infringe Sega's copyrights by operating the BBS, because there was no evidence that the defendant himself was actually uploading or downloading infringing copies. *Id.* at 8. According to the court, whether the defendant was aware that the users of his BBS were infringing Sega's copyright was not relevant on whether the defendant directly caused the copying to occur. The court, however, found the defendant liable on the theory of contributory copyright infringement because defendant

(...continued)

may have done so at some time in the past for a particular purpose. Some boards may allow access by the general public, but may operate "pirate areas," known as sub-boards, for the benefit of only a small subset of its subscribers. These privileged subscribers may obtain access to otherwise closely guarded pirate areas through payment of an access fee.

⁴⁰ On computer bulletin boards, for example, a system operator may offer to subscribers a certain number of "download points" if the subscriber provides to the operator of the system (the "sysop") certain valued computer programs or information. The subscriber may then redeem his or her accumulated points for other programs or for general "download time." For purposes of prosecution, it should not be relevant whether the subscribers "pay" for access privileges in cash or in kind.

knew that his users were uploading and downloading copyrighted computer games, and the operation of the BBS induced, caused, or materially contributed to the infringing activity. *Id.* Of particular importance, the court noted that defendant did more than provide the site facilities for known infringing conduct, he actively solicited users to upload unauthorized games, provided instructions on how to download infringing software and sold copiers to facilitate the downloading of games. *Id.* In a finding relating to the barter issue, the court denied defendant's fair use defense emphasizing that the unauthorized copying of Sega game cartridges caused a substantial adverse impact on the potential market for the copyrighted work. The commercial character of the unauthorized copying weighed against a finding of fair use. *Id.* at 10. The court also found defendant liable for federal trademark infringement. See "CHARGING BOTH CRIMINAL COPYRIGHT AND TRADEMARK VIOLATIONS," p. 68.

e. *The first sale doctrine in criminal cases*

The first sale doctrine is one of the specific statutory restrictions that Congress has placed on the exclusive rights of copyright owners, and it can constitute an issue in criminal copyright prosecutions. Criminal defendants frequently contend that they believed that the works they were selling had been the subject of a legitimate first sale. Moreover, in several instances copyright convictions have been overturned because of inadequacies in the government's proof on this issue. See, e.g., United States v. Goss, 803 F.2d 638 (11th Cir. 1986); United States v. Atherton, 561 F.2d 747 (9th Cir. 1977). For this reason, federal prosecutors should have a clear understanding of the first sale doctrine when considering whether to bring a criminal copyright case.

The first sale doctrine limits the copyright owners "exclusive rights" to authorize or distribute copies of a copyrighted work to the public under 17 U.S.C. § 106(3).⁴¹ It provides that a sale of a "lawfully made" copy terminates the copyright holder's authority to interfere with or control subsequent sales or distributions of that particular copy. 17 U.S.C. § 109(a).⁴² See United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) ("where a copyright owner parts

⁴¹ 17 U.S.C. § 106 provides:

Subject to sections 107 through 120, the owner of [a] copyright under this title has the exclusive rights to do and to authorize any of the following:

(3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease or lending.

⁴² The subsection, entitled "Limitations on exclusive rights: Effect of transfer of particular copy or phonorecord," provides in pertinent part:

Notwithstanding the provisions of section 106(3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.

with title to a particular copy of his copyrighted work, he divests himself of his exclusive right to vend that particular copy." In short, through the first sale doctrine, the first purchaser and any subsequent purchaser of that specific copy of a copyrighted work receives the right to sell, display or dispose of his copy of it. He does not, however, receive the right to reproduce and distribute additional copies made from that work. Thus, if copyright owner A sells a copy of a work to B, B may sell that particular copy without violating the law. But if B makes any unauthorized copies of that work, he violates the law.

Since the first sale doctrine never protects a defendant who makes unauthorized reproductions of a copyrighted work, the first sale doctrine can only be a successful defense to an allegation of copyright infringement by distribution. In such instances, a defendant may argue that he merely redistributed an otherwise authorized and legally made copy of a copyrighted work. It is important to note that the first sale doctrine can be successfully invoked by a defendant only if he has been involved in the distribution of legitimately produced, authorized copies. If copies are unauthorized, the first sale doctrine does not apply. See United States v. Drum, 733 F.2d 1503, 1507 (11th Cir.), cert. denied, 469 U.S. 1061 (1984). "Thus, where the source of copies is unlawful, the doctrine is not implicated." Id. (citing United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) ("[a] pirated copy that is reproduced from the original recording without authorization is plainly not the subject of a first sale.)); see also United States v. Powell, 701 F.2d 70, 72-3 (8th Cir. 1983). Therefore, if B knows that the copies he possesses are unauthorized, he cannot defend an infringement claim by arguing that other, unrelated copies were the subject of a first sale. Accordingly, it may be sufficient to show, as is possible with some types of programs, that the particular program was not licensed to the individual who possessed it. Many software companies keep records of authorized licensees for just this purpose. Note, too, that when the defendant later distributes a legally acquired copy, if he keeps an additional copy, even a "backup" copy, this unauthorized copy can serve as the basis for a charge of infringing reproduction.

Further, the privileges created by the first sale principle do not "extend to any person who has acquired possession of the copy or phonorecord from the copyright owner, by rental, lease, loan, or otherwise, without acquiring ownership of it." See 17 U.S.C. § 109(d). Most computer software is distributed through the use of licensing agreements. Under this distribution system, the copyright holder remains the "owner" of all distributed copies. For this reason, alleged infringers should not be able to establish that any copies of these works have been the subject of a first sale. Thus, if A, the copyright owner, simply loans a copy of his work to B, B obtains no ownership interest in the work and is unable to assert first sale as a defense to an infringement action. This is an important limitation, as the distribution systems for some artistic works, most notably motion pictures and computer software, rely on licensing agreements, leases or other devices to transfer possession of copies of a copyrighted work. Under these distribution systems, the copyright holder remains the "owner" of all distributed copies.

Although courts agree that the first sale principle applies to criminal prosecutions, they do not agree on the burden of proof. Several cases suggest that in criminal copyright prosecutions,

the United States must prove that copyrighted work was not the subject of a first sale. See, e.g., United States v. Sachs, 801 F.2d 839, 842 (6th Cir. 1986); United States v. Powell, 701 F.2d 70, 72 (8th Cir. 1983); United States v. Wise, 550 F.2d 1180 (9th Cir.), cert. denied, 434 U.S. 929 (1977); United States v. Atherton, 561 F.2d 747, 749 (9th Cir. 1977); United States v. Drebin, 557 F.2d 1316, 1326 (9th Cir.), cert. denied, 436 U.S. 904 (1978). Other cases, however, hold that the issue of a first sale is an affirmative defense that must be raised by the defendant. See, e.g., United States v. Larracuente, 952 F.2d 672, 673-4 (2d Cir. 1992) (holding that, as in a civil case, the government need only prove ownership of a valid copyright and unauthorized copying); United States v. Goss, 803 F.2d 638, 643-44 (11th Cir. 1986); United States v. Drum, 733 F.2d 1503, 1507 (11th Cir.), cert. denied, 469 U.S. 1061 (1984).⁴³

(1) Proving absence of first sale

In circuits where the first sale doctrine is considered an element of the offense, demonstrating the absence of a first sale can present significant problems of proof because the evidence on this point may often be circumstantial. Some defendants have argued that the government must completely account for the distribution of all copies of a work in order to carry its burden on this question. This would require, in effect, that the government trace the distribution of every lawful copy of a copyrighted work, an unreasonable burden because the most frequently pirated works also tend to be among the most frequently purchased and widely distributed.

⁴³ The legislative history of the copyright statute supports the view that the first sale doctrine was intended as an affirmative defense to copyright infringement:

During the course of its deliberations . . . the committee's attention was directed to a recent court decision holding that the plaintiff in an infringement action had the burden of establishing that the allegedly infringing copies in the defendant's possession were not lawfully made or acquired. . . . The committee believes that the court's decision, if followed, would place a virtually impossible burden on copyright owners. The decision is also inconsistent with the established legal principle that the burden of proof should not be placed on a litigant to establish facts particularly within the knowledge of his adversary. The defendant in such actions clearly has the particular knowledge of how possession of the particular copy was acquired, and should have the burden of providing this evidence to the court. It is the intent of the committee, therefore, that in an action to determine whether a defendant is entitled to the privilege established by section 109(a) and (b), the burden of proving whether a particular copy was made or acquired should rest on the defendant.

H.R. Rep. No. 1476, 94th Cong., 2d Sess. 1, 80-81, reprinted in 1976 U.S. Code Cong. & Admin. News 5659, 5694-95.

This argument has been consistently rejected by the courts. As stated in United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979):

[T]he government can prove the absence of a first sale by showing that the [copy] in question was unauthorized, and it can establish this proof not only by evidence tracing the distribution of that [copy] but also by circumstantial evidence from which a jury could conclude beyond a reasonable doubt that the recording was never authorized and therefore never the subject of a first sale.

See also, United States v. Sachs, 801 F.2d 839, 843 (6th Cir. 1986); United States v. Drum, 733 F.2d 1503, (11th Cir.), cert. denied, 469 U.S. 1061 (1984); United States v. Whetzel, 589 F.2d 707, 711 (D.C. Cir. 1978).

Evidence of reproduction of unauthorized copies is the best and easiest way of meeting the government's burden under the "first sale" doctrine, whether it presents itself as an element or as an affirmative defense. In cases involving violation of distribution rights, two types of circumstantial proof typically demonstrate the absence of a first sale. First, when a defendant's actions indicate that copies have been obtained illegitimately, a jury may infer that no valid first sale has occurred. See Moore, 604 F.2d at 1232; Whetzel, 589 F.2d at 711. Factors which indicate that copies were obtained illicitly include: sale of copies at a price far below legitimate market value; distribution of copies of inferior quality; and presence of false information on the copies, such as a false address for the manufacturer. See Drum, 733 F.2d at 1503; Whetzel, 589 F.2d at 711 (sale of copies of tapes at night from the back of a truck in a parking lot).

Second, the nature of the distribution system employed by the copyright holder may negate the possibility of a first sale. This is particularly true of copyright cases involving film industry products. In a number of cases the absence of a first sale has been established by showing that the works in question were distributed exclusively through loans and leases. Since the first sale defense is premised on a sale and the transfer of title, evidence that the copyright holder sold no copies of the work effectively negates this claim. Compare United States v. Drebin, 557 F.2d 1316, 1326 (9th Cir.), cert. denied, 436 U.S. 904 (1978) (government proved the absence of first sale through evidence that the copyrighted movies had never been sold or transferred; licenses transferred limited rights for distribution and exhibition of the films for a limited time, which are not "sales" for purposes of the first sale doctrine) with United States v. Atherton, 561 F.2d 747 (9th Cir. 1977) (government failed to prove the absence of first sale of a number of films including "Airport" because, although the copyright owner never "sold" copies, it permitted ABC Television Network to permanently retain copies. These transfers fell within the definition of first sale, and ABC Television could have been the source of the movie copies sold by defendant.). See also United States v. Sachs, 801 F.2d 839 (6th Cir. 1986).

2. Drafting the Indictment

To support felony charges, the government must show that a defendant engaged in the "reproduction or distribution, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, with a retail value of more than \$2,500." 18 U.S.C. § 2319(b)(1). If fewer than ten copies have been copied or distributed, or if the copies have a combined value of less than \$2,500, the offense is a misdemeanor. See 18 U.S.C. § 2319(b)(3). However, because a defendant often makes unauthorized copies of numerous copyrighted works or infringes a number of different rights held by a copyright owner, it is not always easy to draft an indictment that accurately reflects a defendant's actions.⁴⁴ While there are no hard and fast rules, there are a number of general factors that are worth noting.

a. *10 or More Copies*

As a basic matter, while reproducing or distributing ten or more copies of a copyrighted work may constitute a felony violation, a prosecutor should not maximize the number of counts by calculating the total number of infringing acts and dividing by ten. The United States Attorneys' Manual states that in order to promote the fair administration of justice as well as the appearance thereof:

all U.S. Attorneys should charge in indictments and informations as few separate counts as are reasonably necessary to prosecute fully and successfully and to provide for a fair sentence on conviction. To the extent reasonable, indictments and informations should be limited to fifteen counts or less, so long as such a limitation does not jeopardize successful prosecution or preclude a sentence appropriate to the nature and extent of the offenses involved.

U.S.A.M. 9-2.164.

In the simplest cases where the defendant infringed only one type of the same copyrighted work, the defendant should be charged with a single count. This amounts to counting the number of illegal copies made or distributed by the defendant in the requisite period and charging them as a single count in the indictment.

⁴⁴ Drafting decisions are less critical, however, since the advent of the Sentencing Guidelines, as additional acts of infringement, whether charged in one or more counts, are likely to be taken into account as relevant conduct, however charged. See Sentencing Guidelines § 2F1.1 application note 6 ("The cumulative loss produced by a common scheme or course of conduct should be used in determining the offense level, regardless of the number of counts of conviction."). Nonetheless, uniformity in charging copyright infringement cases may avoid challenges to the indictment under theories of duplicity or multiplicity.

However, because the criminal copyright statute does not require that all the copyrights infringed be in the same class or be held by the same copyright owner, a defendant can still be convicted of a felony for reproducing or distributing a total of 10 copies of different copyrighted works, as long as they are of the required value and if done in the specified time. According to the legislative history:

the phrase 'of one or more copyrighted works' is intended to permit aggregation of different works of authorship to meet the required number of copies and retail value. For example, a defendant's reproduction of 5 copies of a copyrighted word processing computer program having a retail value of \$1,300 and the reproduction of 5 copies of a copyrighted spreadsheet computer program also having a retail value of \$1,300 would satisfy the requirement of reproducing 10 copies having a retail value of \$2,500, if done within a 180 day period.

H.R. Rep. No. 997, 102 Cong. 2d Sess., at 6 (1992), reprinted in 1992 U.S. Code Cong. & Admin. News 3569, 3574 (1992).

Where the defendant met the felony minimum by reproducing one class of copyrighted materials (e.g., 10 copies of a copyrighted word processing program having a retail value of \$2,600), and also reproduced 10 copies of another computer program copyrighted by a different author and worth more than \$2,500, he should be charged with two felony counts. The legislative history of the criminal copyright statute and its successive revisions makes clear that the statute seeks to protect each individual's copyrighted work. Therefore, as a general rule, charging a defendant with separate counts for violating each of the different copyrights best reflects the underlying purpose of the statute.

Further, since reproducing a "collective work"⁴⁵ or a "compilation"⁴⁶ constitutes multiple violations of the Copyright Act, and one of its goals is to protect the individual's copyrighted work, it is proper to charge separate infringing acts against each individual victim as separate offenses. Thus, for example, where multiple copies of separate copyrighted works are contained on a single videocassette tape or CD-ROM disk, the statute permits multiple charges, assuming of course that the other requirements of the statute can be met.

⁴⁵ 17 U.S.C. § 101 defines a "collective work" as a "work, such as a periodical issue, anthology, or encyclopedia, in which a number of contributions, constituting separate and independent works in themselves are assembled into a collective whole."

⁴⁶ The copyright statute defines a "compilation" as a "work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship. The term 'compilation' includes collective works." 17 U.S.C. § 101.

Also, computer software is often sold with accompanying instruction manuals. These guides and manuals often are costly to produce and are usually copyrighted. Illegal reproductions of both the software and the instruction manual can and should be charged as two separate counts of infringement.

Another exception to this "one count per work" rule may well lie in the area of sound recordings. The infringement of sound recordings generally involves not one, but two separate acts of infringement -- one for the musical work (i.e., the notes and lyrics) and another for the separately copyrighted public performance of the work. Thus, each type of infringement should be charged in different counts. In addition, some courts have held that the appropriate units of prosecution for infringing a record album can be each individual band or song. See United States v. Taxe, 540 F.2d 961, 966 (9th Cir. 1976), cert. denied, 429 U.S. 1040 (1977).

b. *Retail Value*

In order to charge a felony violation of the criminal copyright statute, the government must also prove that the infringing copies have a total retail value of more than \$2,500. In an era where, for example, even the most basic computer programs often can cost more than \$100, this rarely proves difficult. However, the value of the infringing goods becomes more of an issue in sentencing. See "*Sentencing Guidelines*," *infra*, p. 37.

c. *Equitable charging considerations*

In addition to the statutory elements, equitable factors may affect charging choices. Scarce investigative and prosecutive resources have prompted many offices to set strict monetary thresholds in copyright cases as well as other economic crimes. The guidelines may be keyed to the amount of the defendant's financial gain or the amount of the victim's financial loss. Some United States Attorneys' Offices set guidelines of \$100,000 or more.

Although resources are limited, intellectual property crimes may merit some exceptions to strict dollar thresholds for several reasons. First, guidelines keyed to the amount of a defendant's profit may vastly understate the victim's loss.⁴⁷ Second, copyright prosecutions can be important

⁴⁷ The copyright holder possesses not only the right to reproduce and distribute a given work, but also a limited right to control its distribution and reproduction. This includes protection against diminution in value of a copyrighted work caused by the mere appearance of infringing works in the marketplace. The value of a copyrighted work is diminished by counterfeit copies regardless of the price for the counterfeit item because the victim loses a share of the potential market. In addition, the copyright holder's market share is further diluted by subsequent reproduction and distribution of infringing products. Such harm, though perhaps provable and foreseeable, is not addressed by guidelines
(continued...)

in protecting nascent technologies. Third, because copyright infringement is a federal crime with state preemption, if a defendant is not prosecuted federally, he or she will not be prosecuted at all.

Further, some charging decisions demand careful consideration of the specific rights violated by the defendant. In other words, if the defendant has engaged in the counterfeiting of an existing work, as compared to "bootlegging"⁴⁸ or "piracy,"⁴⁹ serious consideration should be given to charging the defendant even if the conduct does not meet the statutory minimum imposed by the United States Attorney's Office. Counterfeiting is usually more serious than bootlegging and piracy because counterfeiters not only reproduce and distribute the underlying copyrighted work, but also imitate its packaging to make it look like genuine merchandise. Thus, counterfeiting not only detracts from potential market share of the copyright holder, but also may create additional harm by defrauding the consumer and injuring the victim's reputation by leading the consumer to believe that he is purchasing an authentic product.⁵⁰ Often such counterfeiting schemes can be charged both as copyright infringement and trademark counterfeiting. See "CHARGING BOTH CRIMINAL COPYRIGHT AND TRADEMARK VIOLATIONS," infra p. 68.

Another factor to consider when making a charging decision is the extent of the civil remedy. Because both the copyright and trademark schemes create extensive civil remedies for holders of intellectual property rights, prosecutors should consider what civil remedies have already been obtained or may be available, and whether such remedies might be sufficient to deter similar behavior. For example, in the trademark context, the Lanham Act expressly provides for the ex parte seizure of offending material by an aggrieved party, see 15 U.S.C. § 1116, and much

(...continued)

that focus on the initial prices charged or profits made by a defendant for infringing products. Last, the victim may also suffer substantial damage to his or her reputation by having inferior items marketed as genuine licensed products. Thus, it might be appropriate to consider not only the number of infringing items made available or sold, the price at which they were sold, and the normal retail price for non-infringing items, but also the nature of the market to which such infringing items were offered and the threat to potential damage for legitimate items.

⁴⁸ Bootlegging occurs most frequently with sound recordings, and traditionally involves releasing copies of public performances not recorded by the copyright holder. However, no effort is made to "legitimize" the unauthorized recording. Consequently, the buyer usually knows exactly what he is purchasing.

⁴⁹ Piracy involves the unauthorized reproduction or distribution of an existing copyrighted work. See Dowling v. United States 473 U.S. 207, 209 n.2 (1985). Pirated copies, like bootlegged copies, are generally marketed so their illegal nature is obvious to the public. Piracy is by far the most prevalent type of infringement, as it requires only the copying of an existing work through the use of readily available technology such as a tape recorder, videocassette recorder, or computer disk drive.

⁵⁰ During the redrafting of § 2318 in 1981, the drafting committee expressed the position, shared by the Department of Justice, that counterfeiting is a more serious crime than traditional piracy. "Counterfeiting defrauds not only the . . . industries, but also the consumer by leading him to believe that he is purchasing an authentic product." S. Rep. 274, Pub. L. No. 97-180, at 8 (1981).

the same result may be sought by a diligent victim of copyright infringement who is well-versed in extraordinary remedies.⁵¹

The availability of a civil remedy, however, should not be the only factor to consider when making a charging decision. Civil remedies may prove futile under certain circumstances. Infringers may be judgment proof, or may have transferred their money outside the United States. This may be particularly true in software infringement cases, because an infringer can reproduce large numbers of high quality copies with only minimal investment.⁵² In such instances, a criminal sanction may be the only meaningful deterrent. Further, the infringer's actions may be so egregious as to warrant criminal prosecution.

Finally, if infringement continues after entry of a permanent injunction or civil consent decree, civil sanctions clearly have failed. The existence of a previous civil order also supports a charge of criminal contempt under 18 U.S.C. § 401.⁵³

3. Other Possible Charges: Money Laundering and RICO

In 1994, Congress added copyright infringement under 18 U.S.C. § 2319 to the list of violations that constitute "specified unlawful activity" under the money laundering statute, 18 U.S.C. § 1956. Thus, proceeds earned by a defendant from copyright infringement can now form the basis for a charge of money laundering.⁵⁴

⁵¹ David Nimmer has suggested that by combining the Copyright Act's provision for impoundment of infringing articles, 17 U.S.C. § 503(a), with a request under the 1909 Supreme Court rules, and by invoking the All Writs Act, 28 U.S.C. § 1651(a), copyright plaintiffs may be able to obtain a truly *ex parte* seizure order. See Nimmer, *supra* note 18, at 10. Note, however, that the mere fact that an *ex parte* seizure may have been obtained by a victim should not necessarily preclude prosecution. Rather, such might present the opportunity for a relatively simple and cost effective prosecution, since the prosecutor need only subpoena the U.S. Marshal or other party in possession of the seized material to acquire evidence. *Id.*

⁵² In Internet and computer bulletin board cases, a relatively modest expenditure in a personal computer and a modem can result in the reproduction and distribution of hundreds or even thousands of exact duplications of copyrighted works.

⁵³ A defendant may not assert double jeopardy for simultaneous prosecution of a criminal contempt and the underlying offense, even if same act or acts gives rise to both charges. The contempt is separately charged as an offense against the court's jurisdiction, while the underlying offense remains an offense against the laws of the United States. See, e.g., *United States v. Mirra*, 220 F. Supp. 361, 365-66 (S.D.N.Y. 1963) (defendant who threw chair at an Assistant United State Attorney during trial summarily held in criminal contempt, then later charged for same act with assault on a federal officer).

⁵⁴ For a detailed discussion of the elements of money laundering and for Department of Justice policy see U.S.A.M. 9-105.000 and Money Laundering Federal Prosecution Manual, June 1994, Money Laundering Section, (continued...)

This is an important development because the penalties for a violation of § 1956 are substantially greater than for a copyright violation. A violation of § 1956 carries maximum potential of a twenty-year prison sentence and a fine of \$500,000 or twice the amount involved in the transaction. There is also a civil penalty of not more than \$10,000 or the value of the funds involved in the transaction, whichever is greater.

More recently, Congress enacted The Anticounterfeiting Consumer Protection Act of 1996. Pub. L. No. 104-153, 110 Stat. 1386 (1996). The Act, *inter alia*, amended 18 U.S.C. § 1961 to include § 2319 within the definition of "racketeering activity." A violation of RICO carries a maximum penalty of twenty years imprisonment and includes a possible fine of "twice the gross profits or other proceeds" of the racketeering activity. 18 U.S.C. § 1963. In light of the greatly increased penalties under §§ 1956 and 1963, it is strongly recommended that prosecutors consider charging money laundering and a RICO violation in connection with a serious violation of 18 U.S.C. § 2319.⁵⁵

4. Juvenile Prosecutions

Federal criminal law does not permit prosecution of juveniles (defined as those who have not attained their eighteenth birthday, 18 U.S.C. § 5031), absent narrowly defined exceptions. While some of the violations described in this manual may be committed by juveniles, these cases will rarely be prosecuted federally.

Where violators are later found to be juveniles, federal investigators should consider turning over available evidence to state agencies for consideration under state "truth-in-labeling" or "true-name-and-address" laws.⁵⁶ Federal prosecutors may also consider initiating federal *in rem* forfeiture actions against the instrumentalities used by juvenile violators. These *in rem* actions depend only on whether certain property was used to manufacture infringing copies, not on any criminal proceedings. 17 U.S.C. § 509. See "Civil forfeiture," *infra* p. 48.

(...continued)

United States Department of Justice.

⁵⁵ For a detailed discussion of RICO and Department of Justice policy see U.S.A.M. 9-110.00 *et. seq.*

⁵⁶ The federal preemption provision, found at 17 U.S.C. § 301, essentially precludes states from enforcing penalties for copyright violations if the intellectual property at issue falls within the "subject matter of copyright" as defined by federal law and if the claimed property rights are "equivalent to" the exclusive rights provided by federal copyright law. However, state statutes that prohibit the sale of goods failing to bear the true name and address of the manufacturer are a possible alternative to federal enforcement. See "ALTERNATIVE STATE REMEDIES," *infra* p. 50.

5. Penalties for Criminal Copyright Infringement

a. *Statutory penalties*

The penalties available for criminal infringement are found at 18 U.S.C. § 2319. A defendant, convicted for the first time of violating 17 U.S.C. § 506, can be imprisoned for up to 5 years and fined \$250,000 or both for the unauthorized reproduction or distribution, during any 180-day period, of at least 10 copies or phonorecords, or 1 or more copyrighted works, with a retail value of more than \$2,500. 18 U.S.C. §§ 2319(b), 3571(b)(3).

The maximum sentence is increased to 10 years' imprisonment, a \$250,000 fine, or both for defendants who previously have been convicted of copyright infringement under 18 U.S.C. § 2319(b)(1).⁵⁷

Finally, a defendant found guilty of a misdemeanor violation can be sentenced to up to one year imprisonment and fined up to \$100,000. See 18 U.S.C. §§ 2319(b)(3); 3571(b)(5). A misdemeanor violation occurs if the defendant violated rights other than those of reproduction or distribution; if he made or distributed fewer than the requisite number of copies; or if the copies did not meet the statutory minimum value; so long as the other elements of 17 U.S.C. § 506(a) are satisfied.

b. *Sentencing guidelines*

Sentences for the offenses of criminal copyright infringement and trademark counterfeiting are now both determined by reference to § 2B5.3 of the United States Sentencing Commission Guidelines Manual ("Sentencing Guidelines") which sets the Base Offense Level at 6.⁵⁸ It also establishes, as a Specific Offense Characteristic, that if "the retail value of the infringing items exceeded \$2,000," then the guideline level is to be increased by the corresponding number of levels from the table in § 2F1.1 (Fraud and Deceit) which are based on "loss." The Commentary further makes clear that the term "infringing items," as used above, "means the items that violate the copyright or trademark laws (not the legitimate items that are infringed upon)."

⁵⁷ Note that by tying the severest sanction to copyright recidivists, 18 U.S.C. § 2319 introduces an additional element into plea negotiations. In cases involving individual and corporate defendants, prosecutors may wish to press for individual pleas, since those pleas could be used in subsequent prosecutions to enhance a defendant's sentence.

⁵⁸ Effective November 1, 1993, the previous § 2B5.4 (Criminal Infringement of Trademark) was deleted in its entirety and consolidated with § 2B5.3, which now controls criminal infringement of a copyright or trademark. See Sentencing Guidelines Appendix C, amendments 481 and 482.

The Sentencing Guidelines thus unequivocally require consideration of "the retail value of the infringing items." It is not entirely clear, however, what "retail value" means in this context. "Retail value" is usually associated with the sale of the legitimate items because such items are normally sold after considering the manufacturer's suggested retail price, and are distributed through conventional retail channels. By comparison, the "retail value" of infringing items is established by their prices on the black or "thieves'" market.

The background commentary does little to clarify this issue, noting only that "the enhancement is based on the value of the infringing items, which will generally exceed the loss or gain due to the offense." If the retail value of the infringing items is the price at which such products are normally sold by the infringer, however, the resultant amount will not exceed, but will be about the same as defendant's gain. In addition, such an accounting does not adequately reflect the "loss" attributable to the offense, because it reflects only the cost to public consumers, and not the potentially greater loss to sellers of legitimate, non-infringing marks.⁵⁹

Courts in several copyright infringement cases have, at least implicitly, recognized these difficulties, and employed various theories to achieve equitable results. In United States v. Larracuente, 952 F.2d 672 (2d Cir. 1991), for instance, the defendant was convicted of criminal copyright infringement for having trafficked in "bootleg" videotapes of movies. The Second Circuit found that, under U.S.S.G. § 2B5.3, the sentencing court "was correct in applying the guidelines to the normal retail price, rather than the lower bootleg price paid by those who presumably are aware that the copies they are buying are not legitimate." Id. at 674. The court reasoned that "[w]here, as here, unauthorized copies are prepared with sufficient quality to permit their distribution through normal retail outlets, the value of the infringing items is their normal retail price to ultimate consumers who purchase from such outlets." Id.⁶⁰

By contrast, in United States v. Kim, 963 F.2d 65 (5th Cir. 1992), which addressed similar issues under the trademark counterfeiting act, 18 U.S.C. § 2320, the Fifth Circuit determined that the trial court erred in its finding "that the retail value that is intended to be taken into consideration by the guideline § 2B5.4(b)(1) is the retail value of the legitimate item rather than the counterfeit item." Id. at 67 n.3. The Court of Appeals held "that the clear and unambiguous

⁵⁹ The narrow view of "loss" adopted in this portion of the Guidelines fails to recognize the losses suffered by legitimate sellers in the form of lost retail sales. Note that guidelines for similar offenses adopt a broader concept of "loss." See, e.g., U.S.S.G. § 2B1.1 (Larceny, Embezzlement, and Other Forms of Theft) (Commentary, Application Note 2) ("Where the market value is difficult to ascertain or inadequate to measure the harm to the victim, the court may measure loss in some other way, such as reasonable replacement cost to the victim."). See also United States v. Cianscewski, 894 F.2d 74 (3d Cir. 1990) (cost to victim of stolen check is full amount of check, not price at which stolen check is resold); United States v. Wilson, 900 F.2d 1350 (9th Cir. 1990) (stolen documents on black market).

⁶⁰ The court noted, however, that it would be a different question "if the infringing items were of obviously inferior quality and were for that reason distributed to consumers who pay far less than the retail price for authentic items." Larracuente, 952 F.2d at 675. Although a witness for the defense testified that the tapes at issue normally sell for between \$10 and \$15, the trial court credited the prosecution's expert, "who testified that the retail price of the films copied . . . averaged just over \$73." Id.

phrase 'retail value of the infringing items' refers to the counterfeit merchandise. The phrase does not, by its terms, refer to the retail value of genuine merchandise -- the items subject to infringement." *Id.* at 68. The court did not remand the case, however, because while the defendant objected to the use of the retail value of the genuine merchandise, he made no attempt to submit evidence concerning the retail value of the infringing items. The court therefore permitted, as not clearly erroneous, the court's reliance on the probation officer's assessment of value. *Id.* at 69.

c. *Other possible enhancements*

Prior to November 1, 1992, it was uncertain whether the "enhancements" contained under the table in U.S.S.G. § 2F1.1 were applicable in calculating a defendant's sentence for criminal infringement of copyright. Compare *United States v. Hernandez*, 952 F.2d 1110 (9th Cir.) (court upheld trial court's partial reliance on U.S.S.G. § 2F1.1, Application Note 7, to increase the calculation of "loss" under the U.S.S.G. § 2F1.1 table),⁶¹ *cert. denied*, 506 U.S. 920 (1992), with *United States v. Payne*, 952 F.2d 827 (4th Cir. 1991) (it was error to apply a two-level adjustment under U.S.S.G. § 2F1.1(b)(2) to defendant's conviction for counterfeiting). The guidelines have since been amended to make clear that the reference in § 2B5.1 to the table contained in § 2F1.1 applies only to the actual table and not to the entire offense guideline. U.S.S.G. § 1B.5(b)(2).⁶² Thus, it is not appropriate to apply additional enhancements from the commentary to § 2F1.1, notwithstanding that several would seem to often arise in the context of intellectual property violations. See, e.g., U.S.S.G. § 2F1.1(b)(2)(A) (defendant's role involved more than minimal planning); U.S.S.G. § 2F1.1(b)(3)(B) (offense involved a violation of an existing judicial or administrative order).

⁶¹ In *Hernandez*, the Court upheld defendants' convictions and sentences for conspiracy to traffic in counterfeit labels and goods, 18 U.S.C. §§ 371, 2318, 2320, and criminal infringement of a copyright, 17 U.S.C. § 506(a). Upon conviction, the district court arrived at a "probable" or "intended" loss of over \$10,000,000, by multiplying the average market value of a counterfeited tape (\$4) by the number of "J-cards" (2,613,600), used as inserts in the counterfeited tape boxes, that were found in defendants' warehouse. The sentencing court's use of this figure was upheld despite the fact that it greatly exceeded the profit lost by the recording industry. The Court of Appeals upheld defendants' sentences based at least partially on § 2F1.1, Application Note 7, which provides that, consistent with § 2X1.1, "if an intended loss that the defendant was intending to inflict can be determined, this figure will be used if it is greater than the actual loss."

⁶² Subsection U.S.S.G. § 1B1.5(b)(2) provides in full:

An instruction to use a particular subsection or table from another offense guideline refers to the particular subsection or table referenced, and not to the entire offense guideline.

B. TRAFFICKING IN SOUND RECORDINGS OF LIVE MUSICAL PERFORMANCES:
18 U.S.C. § 2319A

In 1994, Congress enacted 18 U.S.C. § 2319A to expressly prohibit the unauthorized trafficking in recordings of live musical performances.⁶³ Pub. L. No. 103-465 § 513(a), 108 Stat. 4974 (1994). This statute is primarily intended for use against the burgeoning trade in "bootlegged" musical recordings. Such cases might otherwise be prosecutable as criminal infringement of the copyrights in the underlying musical compositions. In passing the act, Congress evinced its clear intent that the unauthorized trafficking in bootlegged sound recordings and musical compositions, when done for the purposes of commercial advantage or private financial gain, should be treated as a serious offense.

The statute contains three subsections, each of which protects a different right of the performing artist. Section 2319A(a)(1) prohibits "fixing"⁶⁴ the "sounds" or "images" of a live musical performance, § 2319A(a)(2) prohibits transmitting the "sounds" or "images" of a live

⁶³ 18 U.S.C. § 2319A(a) provides in pertinent part:

(a) Offense - Whoever, without the consent of the performer or performers involved, knowingly and for purposes of commercial advantage or private financial gain -

(1) fixes the sounds or sounds and images of a live musical performance in a copy or phonorecord or reproduces copies or phonorecords of such a performance from an unauthorized fixation;

(2) transmits or otherwise communicates to the public the sounds or sounds and images of a live musical performance; or

(3) distributes or offers to distribute, sells or offers to sell, rents or offers to rent, or traffics in any copy or phonorecord fixed as described in paragraph (1) regardless of whether the fixations occurred in the United States;

shall be imprisoned for not more than 5 years or fined in the amount set forth in this title, or both, or if the offense is a second or subsequent offense, shall be imprisoned for not more than 10 years or fined in the amount set forth in this title, or both.

⁶⁴ "A work is 'fixed' in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration. A work consisting of sounds, images, or both, that are being transmitted, is 'fixed' for the purposes of this title if a fixation of the work is being made simultaneously with its transmission." 17 U.S.C. § 101. See "*Fixed medium of expression*," *supra* p. 8.

musical performance to the public,⁶⁵ and § 2319A(1)(3) prohibits distributing to the public or trafficking in any fixed recording of a live musical performance. Under each subsection, the government must also prove beyond a reasonable doubt that the defendant acted: (1) without authorization from the performer involved; (2) knowingly; and (3) for purposes of commercial advantage or private financial gain. (For a detailed discussion of this element under 18 U.S.C. § 2319, see "*Commercial advantage or private financial gain*," supra p. 24. The maximum penalty for a first-time violation of § 2319A is five years' imprisonment, a \$250,000 fine or both. Defendants who have previously been convicted under this statute may be sentenced to a maximum of 10 years' imprisonment, a \$250,000 fine, or both. 18 U.S.C. § 2319A(a). In addition, the statute provides for mandatory forfeiture and destruction of all infringing items upon a defendant's conviction. 18 U.S.C. § 2319A(b). Copies fixed outside the United States and imported into the United States are also subject to seizure and forfeiture. 18 U.S.C. § 2319A(c). Further, a violation of § 2319A is now specifically listed in 18 U.S.C. § 1961(1)(b) as a "racketeering activity" and is subject to the RICO provisions of the Organized Crime Control Act of 1970. Pub. L. No. 104-153, 110 Stat. 1386 (1996).

C. OTHER TITLE 17 CRIMINAL PROVISIONS PROTECTING COPYRIGHTS

In addition to the prohibition against willful copyright infringement, the Copyright Act also contains three lesser criminal sanctions (found at 17 U.S.C. §§ 506(c), (d) and (e)) which share several characteristics. Unlike 17 U.S.C. § 506(a), which gives rise to civil as well as criminal liability, these three sections proscribe conduct which is not civilly actionable. See Evans v. Continental Homes, Inc., 785 F.2d 897, 912-13 (11th Cir. 1986) (no private right of action exists to enforce 17 U.S.C. § 506(c)). Each offense is an infraction, imposing a maximum fine of \$2,500, is discussed briefly below:

1. Protection of Copyright Notices, 17 U.S.C. §§ 506(c) and (d)

Although it is no longer a prerequisite to receiving protection, there are advantages to placing copyright notices on copies of copyrighted works. The purpose of 17 U.S.C. § 506(c) and (d) is to protect the integrity of these copyright notices. 17 U.S.C. § 506(c) provides that:

Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with

⁶⁵ This subsection was intended to apply to unauthorized transmission of bootleg performances through radio or television and not to the unauthorized reproduction of previously recorded but unreleased performances, i.e., studio outtakes. The latter should be considered for prosecution under the criminal copyright law, 17 U.S.C. § 506(a) and 18 U.S.C. § 2319.

fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than \$2,500.

Thus, § 506(c) prohibits three distinct acts: (1) placing a false notice of copyright on an article; (2) publicly distributing articles which bear a false copyright notice; and (3) importing for public distribution articles which bear a false copyright notice. Any one of these acts, if committed "with fraudulent intent," violates 17 U.S.C. § 506(c).

Additional protection of copyright notices is provided by § 506(d) which provides that:

Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than \$2,500.

2. False Representations in Copyright Applications, 17 U.S.C. § 506(e)

As part of the copyright process, individuals who wish to claim statutory remedies for infringement of a work must file an application for copyright registration with the Register of Copyrights. These applications must identify the copyright claimant, explain how the claimant obtained the work, and identify and describe the work. See 17 U.S.C. § 409(1)-(11). The purpose of § 506(e) is to protect against false copyright applications. This section provides that:

Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than \$2,500.

The government must prove that the defendant (1) knowingly made; (2) a false representation; (3) of a material fact; (4) in a copyright application or any written statement filed in connection with an application.

D. OTHER TITLE 18 OFFENSES

1. Trafficking in Counterfeit Labels, 18 U.S.C. § 2318

There are other criminal statutes aside from the copyright statute that can be used to protect copyrighted works. The most important of these is 18 U.S.C. § 2318, which Congress amended on July 2, 1996, as part of the Anticounterfeiting Consumer Protection Act of 1996.

Pub. L. No. 104-153, 110 Stat. 1386 (1996). This Act enhances the integrity of the copyright system by specifically prohibiting trafficking in counterfeit labels designed to be affixed to phonorecords, copies of computer programs, motion pictures or audiovisual works. It also contains a separate prohibition for trafficking in counterfeit documentation or packaging for computer programs.

Section 2318 is not a copyright statute, and the scope of the protections under the statute is broader than those afforded by the Copyright Act. The predecessor to the current § 2318, for example, clearly encompassed trafficking in counterfeit labels on both copyrighted and uncopied works, see United States v. Sam Goody, Inc., 506 F. Supp. 380, 386 (E.D.N.Y. 1981), and this Act continues that coverage. It is important to note, however, that the legislative history suggests that the statute is intended to be applied to violations involving documentation, packaging or labels for computer programs only if affixed or designed to be affixed to "copies of copyrighted computer programs." H.R. 104-556 at 6, 104th Cong., 2d Sess. (1996).

To obtain a conviction under § 2318, the government must prove five elements. They are:

(1) The defendant was trafficking in labels for phonorecords, motion pictures, audiovisual works or computer programs or the packaging for computer programs. "Traffic" means "to transport, transfer or otherwise dispose of, to another, as consideration for anything of value or to make or obtain control of with intent to so transport, transfer or dispose of." 18 U.S.C. § 2318(b)(2).

(2) The labels were "counterfeit." Counterfeit labels are labels which appear to be genuine when, in fact, they are not. See 18 U.S.C. § 2318(b)(1). The requirement that these labels be counterfeit distinguishes this offense from the "bootlegging" or "pirating" of recordings or tapes. Counterfeit records or tapes are works which are made to appear legitimate. Bootleg or pirated records and tapes are copies with no pretense of legitimacy. (For a further discussion of the differences between bootlegging, piracy, and counterfeiting, see "*Equitable charging considerations*," *supra* p. 33 and p. i. Under 18 U.S.C. § 2318, only trafficking in counterfeit items is prohibited. See United States v. Schultz, 482 F.2d 1179, 1180 (6th Cir. 1973). The legislative history to § 2318 clarifies, however, that this section can be applied when "counterfeiters have simulated 'genuine' labels that have not previously existed," insofar as these simulated labels share the same basic criminal purpose as any counterfeit product -- to defraud the consumer with regard to the authenticity of the product. Pub. L. No. 97-180, at 9 (1981).

(3) The counterfeit label was "affixed or designed to be affixed to a phonorecord, a computer program or documentation or packaging for a computer program, or a copy of a motion picture or other audiovisual work." For purposes of 18 U.S.C. § 2318, the terms "copy," "phonorecord," "computer program," "motion picture" and "audiovisual work" have the meanings given those terms by the copyright statute at 17 U.S.C. § 101. See "*Fixed medium of*

expression," *supra* p. 8. Moreover, the prohibitions of 18 U.S.C. § 2318 include counterfeit labels" designed to be affixed or affixed" to one of these four enumerated categories of works.⁶⁶ Therefore, it is not necessary that the label actually be attached to a work.

(4) The defendant knew the labels were counterfeit. Thus, this is a general intent crime.

(5) The offense occurred in the special maritime or territorial jurisdiction of the United States, involved the use of the mails or facilities of interstate or foreign commerce,⁶⁷ or involved a copyrighted computer program. *See* 18 U.S.C. § 2318(c)(1)-(4).

The maximum penalty for a violation of § 2318 is five years' imprisonment, a \$250,000 fine, or both. *See* 18 U.S.C. § 2318(a). Prosecutors also should consider the applicability of the criminal trademark counterfeiting statute, as labels intended to be affixed to counterfeit works often carry counterfeit reproductions of federally registered trademarks. *See* "CHARGING BOTH CRIMINAL COPYRIGHT AND TRADEMARK VIOLATIONS," *infra* p. 68. Further, a violation of § 2318 now can be a predicate offense under the RICO statute. Pub. L. No. 104-153, 110 Stat. 1386 (1996).

2. Interstate Transportation of Stolen Property, 18 U.S.C. § 2314

Prior to 1985, some prosecutors had also charged a defendant who violated the copyright statute with interstate transportation of stolen property, 18 U.S.C. § 2314, on the theory that the intangible copyright interests that were being violated constituted "goods, wares [or] merchandise" which were "stolen, converted or taken by fraud." *See* 18 U.S.C. § 2314. The Supreme Court, however, rejected this theory in *Dowling v. United States*, 473 U.S. 207 (1985). In *Dowling*, the Court reversed the defendant's conviction for the interstate transportation of copyrighted Elvis Presley records, holding that it was not Congress's intention that § 2314 function as a criminalization of copyright infringement. The Court reasoned that an infringer of a copyright neither assumed physical control over the copyright, nor wholly deprived the owner of its use. The statute "seems clearly to contemplate a physical identity between the items unlawfully

⁶⁶ Prior to being amended, it was unclear whether § 2318 encompassed counterfeit labels affixed to computer software, since computer software is usually classified as a "literary work" under copyright law, *Whelan Associates, Inc. v. Jaslow Dental Library, Inc.*, 797 F.2d 1222, 1234 (3d Cir. 1986), *cert. denied*, 479 U.S. 1031 (1987). However, in some cases these programs may qualify as audiovisual works. They almost certainly qualify as such in the form of video games. *See Red Baron-Franklin Park v. Taito Corp.*, 883 F.2d 275, 278 (4th Cir. 1989), *cert. denied*, 493 U.S. 1058 (1990).

⁶⁷ This provision was intended to expand the reach of the statute beyond the "interstate and foreign commerce" jurisdictional base of the predecessor statute. The third clause was intended to facilitate pendent jurisdiction based upon related claims under the federal copyright law. Pub. L. No. 97-180, at 9-10 (1981).

obtained and those eventually transported, and hence [requires] some prior physical taking of the subject goods." Dowling, 473 U.S. at 216.

3. Mail and Wire Fraud, 18 U.S.C. §§ 1341 and 1343

Whether the Mail and Wire Fraud statutes, 18 U.S.C. §§ 1341 and 1343, can be used to prosecute schemes to defraud that involve the misappropriation of copyrights is unclear. These two statutes broadly forbid the use of the mails or wire communications in connection with "any scheme or artifice to defraud." Relying upon this broad language, some prosecutors have used the Mail and Wire Fraud statutes to prosecute schemes which involve commercial copyright infringement. See, e.g., United States v. Dowling, 739 F.2d 1445 (9th Cir. 1984), rev'd on other grounds, 473 U.S. 207 (1985); Cooper v. United States, 639 F. Supp. 176 (M.D. Fla. 1986). These prosecutions proceeded on the theory that acts of copyright infringement defrauded the copyright owners of their right to receive income and royalties. Dowling, 739 F.2d. at 1448-50; Cooper, 639 F. Supp. at 180.

While recent legal developments have clouded the application of the Mail and Wire Fraud statutes to copyright infringement cases, they have not eliminated these statutes entirely. The defendants in Dowling v. United States, 473 U.S. 207 (1985), who successfully appealed convictions for interstate transportation of stolen property under 18 U.S.C. § 2314, did not challenge their convictions under the Mail and Wire Fraud statutes. See Dowling, 739 F.2d at 1448. The Supreme Court declined to consider this issue sua sponte. Id. at 209 n.1.

Moreover, following the Supreme Court's ruling, at least one court has permitted Mail and Wire Fraud prosecutions which arise out of copyright infringement schemes. In Cooper v. United States, 639 F. Supp. 176 (M.D. Fla. 1986), the court rejected the contention that Dowling precluded any mail and wire fraud prosecutions of copyright infringers. Instead, the court concluded that "Dowling cannot be interpreted so as to remove from the reaches of the Wire Fraud statute a scheme to defraud copyright owners, musicians and the public from the protection afforded by the copyright laws of this country." Id. at 180.

Similarly, the recent Supreme Court rulings which redefined the scope of the Mail and Wire Fraud statutes seem to permit the continued use of these statutes in copyright matters. In 1987, the Supreme Court issued two separate opinions defining the scope of Mail and Wire Fraud statutes in cases that involved the theft of intangible property. United States v. McNally, 483 U.S. 350 (1987), rejected the view that the Mail Fraud statute reached schemes which denied the public the loyal services of government officials. Relying on the legislative history of these

statutes, the Court "read [18 U.S.C. § 1341] as limited in scope to the protection of property rights." *Id.* at 360.⁶⁸

Read broadly, *McNally* might be construed to preclude all prosecutions for schemes to defraud individuals of intangible property like copyrights. In *Carpenter v. United States*, 484 U.S. 19 (1987), however, the Supreme Court made clear that a scheme to defraud the owner of another type of intangible property -- confidential information -- was protected by the Mail and Wire Fraud statutes. Distinguishing *McNally*, the Court stated that, "[c]onfidential business information has long been recognized as property." *Id.* at 26. According to the Court, this intangible interest had received greater legal recognition as property than had the right to honest and faithful services by public employees, a right which the Court characterized as "an interest too ethereal in itself to fall within the protection of the mail fraud statute." *Id.*

The continued use of the Wire and Mail Fraud statutes to successfully prosecute defendants for schemes to defraud which involve theft of copyrighted property has been clouded by *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994). *LaMacchia* operated an electronic bulletin board service (BBS) and permitted users to upload and download copyrighted software at no cost. Because *LaMacchia* did not seek to benefit economically from this scheme, he could not be charged with criminal copyright infringement under 18 U.S.C. § 2319.

The indictment charged *LaMacchia* with conspiracy to commit wire fraud by entering into a scheme to defraud the computer software developers of their rights to reproduce and distribute their product. The district court dismissed the indictment opining that under *Dowling*, "the 'bundle of rights' conferred by copyrights is unique and distinguishable from the indisputably broad range of property interests protected by the mail and wire fraud statutes." *Id.* at 543. The court concluded that *Dowling* precluded *LaMacchia*'s prosecution for conduct that really constituted copyright infringement, albeit not covered by the criminal copyright statute.⁶⁹ *Id.* at 545.

⁶⁸ *McNally* was superseded by 18 U.S.C. § 1346 on the narrow ground of theft of the intangible right of honest services, see *United States v. Stoneman*, 870 F.2d 102 (3rd Cir.), cert. denied, 493 U.S. 891 (1989)); *United States v. Gray*, 96 F.3d 769 (5th Cir. 1996). But see *United States v. Brumley*, 79 F.3d 1430 (5th Cir. 1996) (section 1346 inadequate to restore intangible right of honest and faithful service to purview of Mail and Wire Fraud statutes.)

⁶⁹ The *LaMacchia* court reasoned that while the Wire Fraud statute does reach schemes to defraud someone of an intangible property right, such as a citizen's right to honest government, non-disclosure to the victim can only serve as the basis of a scheme when a defendant has a fiduciary or statutory duty to make an affirmative disclosure. Here, no fiduciary relationship existed between *LaMacchia* and the manufacturers whose software copyrights *LaMacchia* allegedly infringed. Additionally, there was no statutory duty of disclosure because there was no compulsory software licensing scheme similar to the compulsory licensing scheme of the Copyright Act, 17 U.S.C. § 115, which requires vendors to notify copyright owners of the intention to manufacture and distribute protected phonorecords. It was this duty to disclose that formed the basis of the defendant's conviction for fraud in *Dowling*. 871 F. Supp. at 542 - 43.

It is unclear whether the rationale of LaMacchia will be adopted by other courts.⁷⁰ If it is, prosecutors would be precluded from using the Mail and Wire Fraud statutes to charge criminal schemes to defraud which entail, without more, the reproduction and distribution of copyrighted material. However, both statutes could still be used to prosecute schemes to defraud which involve theft of intangible property that is not copyrighted.

4. Smuggling, 18 U.S.C. § 545

Infringing articles are often manufactured overseas and then shipped into the United States for distribution. Commercial importation of unauthorized copies of copyrighted works constitutes copyright infringement. See 17 U.S.C. §§ 501(a) and 602. In such instances prosecutors should consider also charging the defendant with violating 18 U.S.C. § 545 which makes it a felony to import, receive or transport goods "knowing the same to have been imported or brought into the United States contrary to law."

E. STATUTE OF LIMITATIONS

It is important to note that copyright violations have only a three-year statute of limitations. 17 U.S.C. § 507(a) ("[n]o criminal proceedings shall be maintained under the provisions of this title unless it is commenced within three years after the cause of action arose."). See United States v. Shabazz, 724 F.2d 1536, 1540 (11th Cir. 1984) ("In copyright infringement actions, the period of limitation begins on the date of the last infringing act. . . . The trial record reflects the unauthorized duplication of legitimate copyrighted tapes in the same year of the indictment, thereby satisfying the three year Statute of Limitations.") (citations omitted). Although cases brought under Title 18 generally have a five-year statute of limitations, 18 U.S.C. § 3282, prosecutions under 18 U.S.C. § 2319 are subject to the three-year statute of limitations because the underlying prohibition is set out in 17 U.S.C. § 506.

F. FORFEITURE

Federal law also protects copyrights by providing for the forfeiture of both infringing copies and the equipment used to make them. This forfeiture may occur as part of the criminal prosecution or through a separate civil proceeding.

⁷⁰ For a discussion concluding that LaMacchia was wrongly decided see Aaron Hoog, Note, Defrauding the Wire Fraud Statute: United States v. LaMacchia, 8 Harv.J.L. & Tech. 509 (1995).

1. Criminal Forfeiture

Criminal forfeiture is available only after convictions. There are three criminal forfeiture provisions which relate to copyright violations. The most significant one is found at 17 U.S.C. § 506(b) which provides that:

When any person is convicted of [criminal copyright infringement], the court in its judgment of conviction shall, in addition to the penalty therein prescribed, order the forfeiture and destruction or other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords. (Emphasis added.)

Note that this statutory language is mandatory and leaves the judge no discretion.

Section 2318 of Title 18 contains a similar provision, requiring the court to order as part of any judgment of conviction, "the forfeiture and destruction or other disposition of all counterfeit labels and all articles to which counterfeit labels have been affixed or which were intended to have had such labels affixed." See 18 U.S.C. § 2318(d). Note that unlike 17 U.S.C. § 506(b), which requires the forfeiture of the "implements, devices or equipment used" in the offense, the forfeiture mandated by 18 U.S.C. § 2318(d) does not include such devices or equipment, but is limited to counterfeit labels, articles to which those labels have been affixed, and articles to which those labels were intended to have been affixed.

Prosecutors should seek to seize all infringing copies and, in cases under 18 U.S.C. § 506(a), instrumentalities used in their reproduction or manufacture. As a procedural matter, then, search warrant affidavits should cite 18 U.S.C. §§ 506(a) and 2318. In addition, indictments alleging violations of either of these statutes should contain a forfeiture paragraph.

A third forfeiture provision is found at 18 U.S.C. § 2319A(b) and provides for the mandatory seizure, forfeiture and destruction of all infringing items related to trafficking in sound recordings of live musical performances. See "TRAFFICKING IN SOUND RECORDINGS OF LIVE MUSICAL PERFORMANCES: 18 U.S.C. § 2319A," *supra* p. 40.

2. Civil Forfeiture

In addition to forfeiture ordered as part of a judgment of conviction, Title 17 provides for civil forfeiture proceedings. See 17 U.S.C. § 509. These proceedings are entirely distinct from the criminal forfeiture authorized by 17 U.S.C. § 506(b) and 18 U.S.C. § 2318. The government can institute a civil forfeiture action under 17 U.S.C. § 509 as an *in rem* proceeding directed

against the property which has been manufactured or used in violation of the law. Therefore, unlike criminal forfeiture, a civil forfeiture is not dependent on a criminal conviction. Moreover, civil forfeiture proceedings are governed by a lower burden of proof than criminal prosecutions. See 19 U.S.C. § 1615.

Three general classes of property are subject to forfeiture under § 509(a): (1) criminally infringing copies; (2) all plates, masters or molds by which such copies may be reproduced; and (3) all devices used to manufacture, reproduce or assemble such infringing copies. The procedures for seizure, forfeiture and disposition of property, are described in 17 U.S.C. § 509(b). This subsection essentially provides that civil copyright forfeitures are governed by the forfeiture provisions of the customs laws (set forth in 19 U.S.C. §§ 1601 et seq.), which provide for both judicial and administrative forfeitures of seized property.

To institute forfeiture proceeding under 17 U.S.C. § 509, the government must first establish probable cause. Once probable cause is established, the burden shifts to the claimant to show, by a preponderance of the evidence, that the defendant property was not involved in illegal activity. See United States v. One Sharp Photocopier, Model SF-7750, 771 F. Supp. 980, 983 (D. Minn. 1991) (forfeiture of copier used to produce infringing copies of software operations manual).

Prosecutors with questions concerning forfeiture practice and procedure should contact the Asset Forfeiture and Money Laundering Section of the Criminal Division at (202) 514-1263.

G. REPORTING REQUIREMENTS

The Anticounterfeiting Consumer Protection Act of 1996, Pub. L. No. 104-153, 110 Stat. 1386 (1996), requires the Attorney General to provide Congress with detailed information concerning investigations and prosecutions under the criminal intellectual property statutes, 18 U.S.C. §§ 2318, 2319, 2319A, and 2320. 18 U.S.C. § 2320(e).⁷¹

⁷¹ Section 2320(e), as amended by the Anticounterfeiting Consumer Protection Act of 1996, Pub. L. No. 104-153, 110 Stat. 1386 (1996), provides as follows:

(e) Beginning with the first year after the date of enactment of this subsection, the Attorney General shall include in the report of the Attorney General to Congress on the business of the Department of Justice prepared pursuant to section 522 of title 28, an accounting, on a district by district basis, of the following with respect to all actions taken by the Department of Justice that involve trafficking in counterfeit labels for phonorecords, copies of computer programs or computer program documentation or packaging, copies of motion pictures or other audiovisual works (as defined in section 2318 of title 18), criminal infringement of copyrights (as defined in section 2319 of title 18), unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances (as defined in section 2319A of title 18), or trafficking in goods or services bearing counterfeit marks (as defined in section 2320 of title 18):

(continued...)

H. ALTERNATIVE STATE REMEDIES

The federal preemption provision, found at 17 U.S.C. § 301, essentially precludes the states from enforcing penalties for copyright violations if the intellectual property at issue falls within the "subject matter of copyright" as defined by federal law and if the claimed property rights are "equivalent to" the exclusive rights provided by federal copyright law. See Gencraft Homes Inc. v. Sumurdy, 688 F. Supp. 289 (E.D. Tex. 1988). Thus it appears that in most instances criminal prosecution for copyright infringement is possible only under federal law. See "Historical Grounds for Copyright Protection," supra p. 5.

This federal preemption has resulted in an enforcement gap, at least in cases that are deemed insufficient to warrant federal enforcement and prosecutive resources. State statutes that prohibit the sale of goods failing to bear the true name and address of the manufacturer are a possible alternative to federal enforcement. These laws, generically known as "truth-in-labeling" laws or "true-name-and-address" statutes, currently exist in 43 states, and can often support "street market" or "flea market" raids to seize infringing articles that might otherwise escape federal prosecution. Prosecutors are urged to consider referrals to state law enforcement agencies in cases that might not warrant federal resources. See APPENDIX L for a list of state "true-name-and-address" statutes.

(...continued)

- (1) The number of open investigations.
- (2) The number of cases referred by the United States Customs Service.
- (3) The number of cases referred by other agencies or sources.
- (4) The number and outcome, including settlements, sentences, recoveries, and penalties, of all prosecutions brought under sections 2318, 2319, 2319A, and 2320 of title 18.

18 U.S.C. § 2320(e).

IV. PROTECTION OF TRADEMARKS

A. INTELLECTUAL PROPERTY ENTITLED TO TRADEMARK PROTECTION

Trademarks originated in medieval times to identify certain goods as the products of particular craftsmen. Today, courts recognize and protect four functions performed by trademarks. These are:

- (1) identifying a particular seller's goods and distinguishing them from goods sold by others;
- (2) signifying that all goods bearing the trademark come from or are controlled by a single source;
- (3) signifying that all goods bearing the trademark are of an equal level of quality; and
- (4) as a prime instrument in advertising and selling the goods.

1 J. THOMAS MCCARTHY, McCarthy on Trademarks and Unfair Competition § 3.01[2] (1995) (hereinafter McCarthy). A trademark is also an important "objective symbol of the good will that a business has built up. Without the identification function performed by trademarks, buyers would have no way of returning to buy products that they have used and liked." Id. Thus, trademarks (a term used here to include service marks)⁷² are used not only to identify sources of goods, but also to obtain marketing advantage.

1. Constitutional Limits on Trademark Protection

Unlike copyrights and patents, Congress's power to regulate trademarks rests on no specific Constitutional grant. The Supreme Court has ruled that the patent and copyright clause of the Constitution does not apply to trademarks. Trade-Mark Cases, 100 U.S. 82 (1879).⁷³ The Supreme Court found "insurmountable difficulties" in attempting to classify "essential characteristics" of a trademark as inventions and discoveries, or as writings of authors. A

⁷² "Service marks" are trademarks which identify a service as opposed to a product.

⁷³ That clause grants to Congress the power "[t]o promote the Progress of Science and the useful Arts, by securing for Limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. CONST. art. I, § 8, cl. 8.

trademark "require[s] no fancy or imagination, no genius, no laborious thought. It is simply founded on priority of appropriation." Id. at 94.

Therefore, Congress's power to regulate trademarks comes from the Commerce Clause of the Constitution which grants Congress the power "to regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes." U.S. CONST. art. I, § 8, cl. 3. Thus, Congress may exercise its power to regulate marks only in interstate or foreign commerce. See 15 U.S.C. § 1051 et seq.

2. Nature of the Rights Protected by Trademarks

Both state and federal law provide trademark owners with remedies against infringement. State laws often are based on the tort concepts of "passing off" and "dilution." Federal trademark law is contained in the Lanham Act, 15 U.S.C. § 1051 et seq., which provides that the owner of a trademark has the exclusive right to use the mark, or license it. A trademark owner also has the right to prevent the use of confusingly similar marks by unauthorized third parties. The owner of a mark on the principal register of the United States Patent and Trademark Office can seek civil remedies against a counterfeiter, 15 U.S.C. § 1116(d), or block importation of infringing goods, U.S.C. § 1124. Criminal remedies are provided for by 18 U.S.C. § 2320.

3. Statutory Limits on Trademark Protection

Federal trademark law, unlike federal laws preempting and controlling patents and copyrights, coexists with state and common-law trademark rights. Ownership of a mark arises not through any single act of federal registration, but rather through continued use. Registration of a mark with the Patent and Trademark Office, however, offers a number of procedural and substantive legal advantages over reliance on common law rights. For example:

(1) a registrant has access to the federal courts without pleading any required amount in controversy, 15 U.S.C. § 1121;

(2) in federal court, lost profits, damages and costs are recoverable, and treble damages and attorney fees are available, 15 U.S.C. § 1117;

(3) evidence of registration is "prima facie evidence of the validity of the registered mark, . . . of the registrant's ownership of the mark, and of the registrant's exclusive right to use the registered mark. . . ." 2 McCarthy, § 19.05 (1995). 15 U.S.C. § 1057(b); and

(4) registration may be used to establish priority of trademark rights, as the registration would specify either the date of first use in commerce, 15 U.S.C. § 1051(a), or the date of the intent to use the mark in commerce. 15 U.S.C. § 1051(b).⁷⁴

Most important for prosecutors, federal registration is a jurisdictional prerequisite to federal criminal prosecution and is an essential element in a prosecution for trademark counterfeiting. 18 U.S.C. § 2320. The government must show that the genuine mark was registered on the principal register in the United States Patent and Trademark Office. See U.S.A.M. 9-68.331(D). To register a trademark on the principal register, the owner must establish (i) distinctiveness of the mark, and (ii) use or intent to use the mark in interstate or foreign commerce. 18 U.S.C. § 1052.

a. *Distinctiveness*

A finding that a trademark is "distinctive" does not represent a judgment on the trademark's quality. Rather, trademarks must be distinctive in roughly the same way that copyrights must be original: "[n]o trademark by which the goods of the applicant may be distinguished from the goods of others shall be refused registration." 15 U.S.C. § 1052. Trademarks may be inherently distinctive,⁷⁵ non-inherently distinctive,⁷⁶ or descriptive.⁷⁷ This distinction is important because non-inherently distinctive trademarks are protected only if they have acquired secondary meaning.⁷⁸ See generally Abercrombie & Fitch Co. v. Hunting World,

⁷⁴ For a complete list of the advantages that federal registration offers, see 2 McCarthy, § 19.05 (1995).

⁷⁵ Distinctive trademarks are trademarks such as "Exxon" that immediately serve as an identifier of the source of the product. See, e.g., Taco Cabana Int'l v. Two Pesos, Inc., 932 F.2d 1113, 1120 n.7 (5th Cir.), aff'd, 505 U.S. 763 (1992).

⁷⁶ Trademarks that are non-inherently distinctive are not sufficiently "distinctive" to be automatically eligible for federal registration, but are eligible for registration if they have become distinctive through use.

⁷⁷ A mark is "descriptive" if it is descriptive of (i) the intended purpose, (ii) function or use of the goods, (iii) the size of the goods, (iv) the class of users of the goods, (v) a desirable characteristic of the goods or (vi) the end effect upon the user. 1 McCarthy, § 11.05[2] (1995). A descriptive mark is usually accorded a narrow scope of exclusivity and is therefore deemed to be a weak mark.

⁷⁸ Secondary meaning for a descriptive term is a matter of fact, to be determined from relevant evidence probative of probable customer reaction. 1 McCarthy, § 11.09 (1995). According to McCarthy, "the Supreme Court of North Carolina gave an excellent capsule definition of secondary meaning in the context of descriptive terms:"

When a particular business has used words *publici juris* so long or so exclusively or when it has promoted its product to such an extent that the words do not register their literal meaning on the public mind but are instantly associated with one enterprise, such words have attained a secondary

(continued...)

Inc., 537 F.2d 4 (2d Cir. 1976). The requirement that trademarks be distinctive prohibits registering generic marks, i.e., common commercial names for goods.

Of course, claims that a trademark is distinctive must always be considered in conjunction with the goods or services for which the mark is sought. Thus, the word "apple" cannot be registered to a single apple orchard, since it is a generic name for the items produced and could never be distinctive in that context. The same may initially be true if the mark "apple" were claimed by a gum or candy manufacturer, because the term directly classifies the flavor of the manufacturer's products and those of others. Consequently it would fail to identify any single source.⁷⁹ Yet the word "apple," although generic or generally descriptive in certain contexts, is arbitrary or fanciful for computer products, and has been accordingly registered as a trademark.

b. *Use in commerce*

The Lanham Act only allows registration of marks "used in commerce," which means:

the bona fide use of a mark in the ordinary course of trade, and not made merely to reserve a right in a mark. For purposes of this [Act], a mark shall be deemed to be in use in commerce -

...

on services when it is used or displayed in the sale or advertising of services and the services are rendered in commerce, or the services are rendered in more than one State or in the United States and a foreign country and the person rendering the services is engaged in commerce in connection with the services.

The word "commerce" means all commerce which may lawfully be regulated by Congress. 15 U.S.C. § 1027.

(...continued)

meaning. That is to say, a secondary meaning exists when in addition to their literal, or dictionary meaning, words connote to the public a product from a unique source.

Id. quoting Charcoal Steak House of Charlotte, Inc. v. Staley, 263 N.C. 199, 139 S.E.2d 185 (1964) ("CHARCOAL STEAK HOUSE" held descriptive; nonsuit affirmed on basis of no likelihood of confusion).

⁷⁹ Such a mark may, however, be capable of acquiring distinctiveness if a manufacturer is able to show that apple gum were to be uniquely identified with one particular producer.

4. Limitations on Exclusive Rights

A trademark can be registered with the United States Patent and Trademark Office for an initial period of ten years, and must be renewed every ten years thereafter. Between the fifth and sixth years of the initial registration period, the registrant must file an affidavit stating that the mark is in use in commerce. Failure to file such an affidavit results in the automatic cancellation of the registration "at the end of six years following the date of registration." 37 C.F.R. § 2.161.

A previously used mark may be legally appropriated if it has been abandoned by an earlier owner. Abandonment results when there is nonuse of the mark, accompanied by an intent to discontinue use.⁸⁰ In addition, public or common use of the mark in the public domain may undercut the distinctive nature of a popular mark. Such a mark may then become the common commercial name or generic name of the goods, as opposed to a source indicator for those goods. For example, the words "aspirin" and "escalator" were, at one time, registered trademarks that have since fallen into public usage. See, e.g., Bayer Co. v. United Drug Co., 272 F. 505 (S.D.N.Y. 1921). Companies that own marks like "Xerox" and "Jeep" expend considerable effort each year to avoid a similar fate. Since the viability of criminal charges may turn on determinations such as these, investigators and prosecutors contemplating criminal charges under § 2320 must confirm the continuing validity of the mark that is counterfeited.

B. THE CRIMINAL LAW

1. Overview of Statute

The Trademark Counterfeiting Act, 18 U.S.C. § 2320, provides that:

- (a) Whoever intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services shall, if an individual, be fined not more than \$2,000,000 or imprisoned not more than 10 years, or both, and, if a person other than an individual, be fined not more than \$5,000,000.

⁸⁰ Two years of continuous non-use is presumptive of abandonment, but the presumption can be rebutted by proof of lack of intent to abandon. Thus, if nonuse results because of economic pressures -- but not as a result of intent to discontinue use -- the nonuse may be excused and held not to constitute abandonment.

2. Elements

In order to establish a criminal offense under 18 U.S.C. § 2320, the government must prove that:

- (1) the defendant trafficked or attempted to traffic in goods or services;
- (2) such trafficking, or attempt to traffic, was intentional;
- (3) the defendant used a "counterfeit mark" on or in connection with such goods or services; and
- (4) the defendant knew that the mark so used was counterfeit.

Conspiracies to violate the Act can be prosecuted under 18 U.S.C. § 371. United States v. Yamin, 868 F.2d 130 (5th Cir.), cert. denied, 492 U.S. 924 (1989).

a. *Trafficked in goods or services*

The term "traffic" is defined in 18 U.S.C. § 2320(d)(2) to mean "transport, transfer, or otherwise dispose of, to another, as consideration for anything of value, or make or obtain control of with intent so to transport, transfer or dispose of." This definition is broad enough to cover all aspects of commercial activity from initial manufacture to sale to the ultimate purchasers. However, the knowing purchase of goods bearing counterfeit marks for the purchaser's personal use is not covered by § 2320. See Joint Statement on Trademark Counterfeiting Legislation, 130 Cong. Rec. H12076, H12078, 98th Cong., 2d Sess. (daily ed. Oct. 10, 1984) (hereinafter "Joint Statement"); see also U.S.A.M. 9-68.310.

b. *Trafficking was intentional*

The first of two mens rea elements is that the defendant's trafficking was "intentional"; that is, that he or she acted deliberately or "on purpose." See U.S.A.M. 9-68.320; Joint Statement at H12076. The statute does not require, however, a specific intent to violate the statute. See United States v. Baker, 807 F.2d 427, 429 (5th Cir. 1986) (rejecting defendant's claim that, "even though he had the mental states required by the statute, he should not be convicted because he did not know that Congress had passed a statute criminalizing his conduct."); United States v. Gantos, 817 F.2d 41, 42-43 (8th Cir.), cert. denied, 484 U.S. 860 (1987).

c. *The defendant used a "counterfeit mark"*

The term "counterfeit mark" is defined in the criminal statute, 18 U.S.C. § 2320(d)(1), and in the Lanham Act, 15 U.S.C. § 1127. Although the definitions differ slightly for technical reasons, they are intended to be identical in substance. Joint Statement at H12078. The United States Attorney's Manual identifies seven requirements of a counterfeit mark, U.S.A.M. 9-68.331(A-G).⁸¹

(1) The mark is "spurious." A mark is "spurious" if it is "not genuine or authentic." Joint Statement at H12078.

(2) The mark was used in connection with goods or services. 18 U.S.C. § 2320(d)(1)(A)(I).

(3) The counterfeit mark is "identical with, or substantially indistinguishable from" the genuine trademark. 18 U.S.C. § 2320(d)(1)(A)(ii). The phrase "substantially indistinguishable from" is intended to prevent a counterfeiter from escaping liability by modifying a protected trademark in trivial ways. At the other end, it also serves to exclude the arguable case of trademark infringement that is merely "reminiscent of" protected trademarks. Joint Statement at H12078; U.S.A.M. 9-68.331.

(4) The genuine mark is registered on the principal register in the United States Patent and Trademark Office. 18 U.S.C. § 2320(d)(1)(A)(ii).

(5) The genuine mark is in use. The genuine mark must not only be registered, it must also be in use. 18 U.S.C. § 2320(d)(1)(A)(ii).

(6) The goods or services are those for which the genuine mark is registered. The definition of a counterfeit mark extends only to imitations of registered marks that are used in connection with the goods or services for which the mark is registered. See 18 U.S.C. § 2320(d)(1)(A)(i), (ii). "For example, a mark used in connection with typewriter paper which is identical to or substantially indistinguishable from a mark registered only for use on typewriters would not be a counterfeit mark, although civil remedies might be available under the Lanham Act." U.S.A.M. 9-68.331.

(7) The use of the counterfeit mark is "likely to cause confusion, to cause mistake, or to deceive." The phrase "use of which is likely to cause confusion, to cause mistake, or to deceive" is taken from the Lanham Act, 15 U.S.C. § 2320(d)(1)(A)(iii), and is intended to insure that no

⁸¹ The Act also covers trademarks protected by the Olympic Charter Act. The designations protected are set forth at 36 U.S.C. § 380.

conduct will be criminalized which does not constitute trademark infringement under the Lanham Act. Joint Statement at H12079.

The likelihood of confusion is a question of fact for the jury. United States v. Gonzalez, 630 F. Supp. 894 (S.D. Fla. 1986). However, criminal courts have adopted a number of factors used in the civil context when analyzing whether there is a likelihood of confusion between two marks. United States v. Torkington, 812 F.2d 1347, 1354 (11th Cir. 1987); United States v. McEvoy, 820 F.2d 1170, 1172 (11th Cir.), cert. denied, 484 U.S. 902 (1987). These factors, which may be argued to a jury in a criminal case, Torkington, 812 F.2d at 1354, include the type of trademark, the similarity of design, the similarity of product, identity of retailers and purchasers, similarity of advertising media used, the defendant's intent, and any actual confusion engendered.

Generally, the test is whether an average consumer would be deceived into thinking that the product was made by the genuine trademark owner. See Montres Rolex, S.A. v. Snyder, 718 F.2d 524, 530-32 (2d Cir. 1983), cert. denied, 465 U.S. 1100 (1984). Where counterfeit goods are involved in criminal cases under § 2320, the trier of fact may decide whether likelihood of confusion is likely either through a side by side comparison of products, through expert testimony, or both. See United States v. Yamin, 868 F.2d 130 (5th Cir.), cert. denied, 492 U.S. 924 (1989); Rolex Watch USA, Inc. v. Canner, 645 F. Supp. 484, 489 (S.D. Fla. 1986).

The "likely to cause confusion" test may also be satisfied by a showing that it is likely that members of the public would be "confused, mistaken or deceived should they encounter the allegedly counterfeit goods in a post-sale context." Torkington, 812 F.2d at 1352. Because subsequent purchasers or recipients of the goods may be duped, it is not a defense that the original buyer was told that the goods were counterfeit; nor is it a defense that the buyer was actually not confused because of the comparatively low price of the fake goods. Id. at 1350. See also United States v. Gantos, 817 F.2d 41, 43 (8th Cir.) (a "counterfeit" is not limited to goods which deceive only the immediate purchaser; the fact that the defendant told the buyer that the "Rolex" watches were counterfeit does not make them any the less counterfeit), cert. denied, 484 U.S. 860 (1987); United States v. Hon, 904 F.2d 803, 806 (2d Cir.) ("an interpretation of § 2320's confusion requirement to include the non-purchasing public advances the important purpose underlying the trademark laws of protecting the trademark owner's investment in the quality of the mark and his product's reputation. . . ."), cert. denied, 498 U.S. 1069 (1991).

d. *The defendant knew that the mark was counterfeit*

The government must also prove that the defendant "knew" that the mark used on or in connection with trafficked goods or services was counterfeit. See U.S.A.M. 9-68.340. This element requires proof of actual knowledge of the counterfeit nature of the mark, defined in the

Joint Statement as "an awareness or a firm belief to that effect." Joint Statement at H12076. "Thus, a manufacturer who believes in good faith that he or she has a prior right to use a particular mark, or that a mark does not infringe a registered mark, could not be said to 'know' that the mark is counterfeit." Joint Statement at H12077. This burden can be met, however, by demonstrating that the defendant was "willfully blind" to the counterfeit nature of the mark. See Joint Statement at 12077; see also United States v. Sung, 51 F.3d 92, 94 (7th Cir. 1995) (vendor is under duty to inquire into the status of the mark); United States v. Jewell, 532 F.2d 697 (9th Cir.), cert. denied, 426 U.S. 951 (1976). This showing can be made through circumstantial evidence regarding the defendant's purchase of the goods, the method of delivery, packaging conventions, and an unusually low price. Knowledge of the criminality of the conduct is not an element of the offense. United States v. Baker, 807 F.2d 427 (5th Cir. 1986).

3. Defenses

a. *Lanham Act defenses*

"All defenses, affirmative defenses, and limitations on remedies which would be applicable in an action under the Lanham Act for trademark infringement are applicable for trafficking in counterfeit goods under 18 U.S.C. § 2320." 18 U.S.C. § 2320(c). Incorporating all civil defenses into the criminal statute insures that no person will be found criminally culpable of trademark counterfeiting if he could have successfully defended a civil infringement action. U.S.A.M. 9-68.400.

Under the Lanham Act, defenses include laches, unclean hands, fraud in obtaining trademark registration, or use of the mark in violation of the antitrust laws. Possible defenses may also involve a challenge to the continuing validity of the trademark infringed: the mark may not be properly registered, may have been abandoned or may have fallen into common or generic usage.

Where such defenses are raised, case law under the Lanham Act, 15 U.S.C. § 1051 *et seq.*, may prove instructive. As a general rule, however, cases that provide an opportunity for a defendant to colorably raise such defenses should not be prosecuted criminally.

b. *Overrun or "grey market goods"*

The statute expressly excludes from the definition of "counterfeit mark" any items commonly termed "overrun goods," which are:

goods or services of which the manufacturer or producer was, at the time of the manufacture or production in question authorized to use the mark or designation for the type of goods or services so manufactured or produced, by the holder of the right to use such mark or designation.

18 U.S.C. § 2320(d)(1)(B).⁸²

The legislative history provides an example: if a licensee was authorized to make 500,000 umbrellas bearing a trademark owner's mark and the licensee manufactured without authorization an additional 500,000 umbrellas bearing that mark during the course of the license, the contractual and other civil remedies already existing make it inappropriate to criminalize such practices. Joint Statement at H12077.

The overrun exclusion cannot be claimed, however, where a licensee produces a type of good other than the one for which he is licensed. For example, "if a licensee is authorized to produce 'Zephyr' trenchcoats, but without permission manufactures 'Zephyr' wallets,' the overrun exception would not apply." *Id.* The legislative history also makes clear that the burden is on the defendant to prove that the goods or services in question fall within the overrun exclusion.

4. Charging Decisions

As the following discussion demonstrates, most charging issues are parallel to those raised in criminal copyright cases. See "Drafting the Indictment," *supra* p. 31.

a. *Intent of statute*

Before the Anti-Counterfeiting Act of 1984, there were no federal criminal penalties for trademark counterfeiting. Congress enacted this section in response to an increase in commercial trademark counterfeiting and it reflects an intention to impose stiff criminal penalties upon intentional acts that were previously subject only to civil sanctions under the Lanham Act.

⁸² Also excluded from the definition of counterfeit mark are so-called "parallel imports" or "grey market" goods, which are trademarked goods legitimately manufactured and sold overseas and then imported into the United States outside of the trademark owner's traditional distribution channels. Thus the criminal statute cannot be used to reach those who traffic in goods that were produced by a licensed manufacturer at the time that the license was valid, even if the goods were then sold at a time when the license was not. See Joint Statement at 12079. Neither is the statute intended to apply to mere imitations of "trade dress," such as the color, shape, or design of a product or its packaging -- unless such features are also registered as trademarks.

"Congress was concerned not only that '[t]rademark counterfeiting . . . defrauds purchasers, who pay for brand-name quality and take home only a fake,' but also that 'counterfeiters [can earn] enormous profits . . . by capitalizing on the reputations, development costs, and advertising efforts of honest manufactures at little expense to themselves.'" United States v. Hon, 904 F.2d 803, 806 (2d Cir. 1990)(citation omitted), cert. denied, 498 U.S. 1069 (1991).⁸³

b. *Money laundering/RICO*

In 1994, Congress added trademark counterfeiting under 18 U.S.C. § 2320(c)(7)(D) to the list of violations that constitute "specified unlawful activity" under the money laundering statute, 18 U.S.C. § 1956. Thus, proceeds earned by a defendant from trafficking in counterfeit goods can now form the basis of a money laundering charge. This is an important development because the penalties for violations of § 1956 and § 1961 are substantially greater than for trafficking in counterfeit goods. A violation of § 1956 carries a maximum sentence of twenty years in prison and a fine of \$500,000 or twice the amount involved in the transaction. There is also a civil penalty of up to \$10,000 or the value of the funds involved in the transaction, whichever is greater.⁸⁴ Additionally, on July 2, 1996, Congress amended § 1961 to include § 2320 as a RICO predicate offense. A violation of RICO carries a maximum penalty that includes twenty years' imprisonment and a fine of up to "twice the gross profits or other proceeds" of the racketeering activity. 18 U.S.C. § 1963. In light of the greatly increased penalties under §§ 1956 and 1963, prosecutors should consider whether a case involving trafficking in counterfeit goods might support money laundering charges under § 1956 and/or a RICO count.⁸⁵

c. *Equitable charging considerations*

Victims of trademark counterfeiting can also turn to civil remedies that are among the most powerful afforded under our civil law (including ex parte seizure of a defendant's infringing products and treble damage recovery for willful acts of infringement), a factor to consider when determining whether a criminal charge is appropriate. Indeed, the decision to charge or decline a

⁸³ See also Brian J. Kearney, The Trademark Counterfeiting Act of 1984: A Sensible Legislative Response to the Ills of Commercial Counterfeiting, 14 Fordham Urb. L.J. 115, 119-120 (1986).

⁸⁴ For a detailed discussion of the elements of money laundering and for Department of Justice policy see U.S.A.M. 9-105.000 and Money Laundering Federal Prosecution Manual, June 1994, Money Laundering Section, United States Department of Justice.

⁸⁵ For a detailed discussion of RICO and Department of Justice policy see U.S.A.M. 9-110.00 et. seq

criminal case for trademark counterfeiting (as with criminal copyright cases under § 2319, see "*Equitable charging considerations*," supra p. 33) turns on a number of equitable factors.

(1) Extent of civil recovery

At the time Congress enacted § 2320, it also amended the Lanham Act, 15 U.S.C. §§ 1051 et seq., to create new civil remedies: treble damages or the amount of defendant's profits (whichever is greater), attorney's fees, and ex parte seizure of counterfeit goods and instrumentalities under certain circumstances. 15 U.S.C. § 1116(d). As with copyright cases, however, an ex parte civil seizure or a treble damage award should not necessarily foreclose a criminal prosecution. After all, damages awarded in a civil judgment cannot always be collected. In cases where counterfeiters cannot satisfy a civil judgment because they do not have the money, or especially when they have hidden funds or transferred them overseas, criminal prosecution might be warranted.

(2) Violation of existing civil order -- contempt

Criminal charges may also be warranted if counterfeiting continues after entry of a permanent injunction or consent decree in a civil case. These facts strongly suggest that civil remedies will not deter the infringement and that the defendant may regard civil penalties as a cost of doing business. The existence of a civil order also allows a prosecutor to consider bringing a charge of criminal contempt under 18 U.S.C. § 401, in lieu of or in addition to separate criminal charges.

d. *Monetary damages*

As noted in the section on charging decisions in criminal copyright cases, see "*Equitable charging considerations*," supra p. 33, strict adherence to monetary thresholds may be inappropriate in evaluating trademark infringement cases if the most obvious consequences stemming from the defendant's conduct understates the true harm. This is especially true where the charging guidelines refer only to the trafficker's profits and not the economic harm done to the trademark owner. Instead, charging standards should take several factors into account: (1) the amount of loss by all of the victims, including diminution of market share; (2) the total number of counterfeit goods manufactured or sold; (3) the quality of the infringing goods; (4) the price at which they were sold; (5) the normal retail price for non-infringing goods; (6) the market to which such infringing products were sold; and (7) the impact of the items' release on potential demand for the legitimate goods.

e. *Units of prosecution*

In drafting the indictment in a trademark counterfeiting case, the prosecutor should consider the individual marks counterfeited as the proper unit of prosecution. Thus, the trafficking of goods bearing different counterfeited marks should be charged in separate counts. In *United States v. Song*, 934 F.2d 105 (7th Cir. 1991), the court upheld the defendant's conviction on five separate crimes charged in five separate counts "because she was trafficking in goods bearing five different counterfeit marks." *Id.* at 109. The court based its determination on plain language of § 2320 which covers someone who "intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on such goods or services." *Id.* at 108 (emphasis in original).⁸⁶

The charging determination is, of course, subject to a rule of reason, and generally the best approach is to organize charges around a single course of conduct to avoid confusing the jury. As in copyright cases, prosecutors must consider the number of separate victims affected by the crimes. However, if charging separate counts for each victim would produce an unwieldy indictment, prosecutors may choose to group each offense by category, such as, for example, the date upon which the goods were manufactured, distributed, or seized. Indictments charging counterfeiting and trafficking schemes can be unified through a conspiracy count under 18 U.S.C. § 371.

f. *Juvenile prosecutions*

Federal criminal law does not permit the prosecution of juveniles (defined as those who have not attained their eighteenth birthday, 18 U.S.C. § 5031), absent narrowly enumerated exceptions. It is unlikely a violation of 18 U.S.C. § 2320 will meet these limited exceptions. Where violators are discovered to be juveniles, federal investigators should consider turning over available evidence to state agencies for evaluation under state laws.

⁸⁶ The court in *Song* did not address cases where a vendor sold different types of goods, some of which might carry the same counterfeit mark.

C. PENALTIES

1. Statutory

In 1994, Congress revised the penalties under § 2320 to now carry a possible 10-year prison term or a fine of up to \$2,000,000, or both, for first-time offenders. Pub. L. No. 103-322, 108 Stat. 2110, 2148 (1994). In addition, a subsequent conviction carries a prison term of up to 20 years, a \$5,000,000 fine, or both. These revisions also raised the first offender corporate fine from \$1,000,000 to \$5,000,000. Recidivist corporations may be fined up to \$15,000,000.

2. Sentencing Guidelines

Sentences for trademark counterfeiting and for copyright violations are now both determined by reference to U.S.S.G. § 2B5.3 which sets the Base Offense Level at 6.⁸⁷ See "*Sentencing Guidelines*," *supra* p. 37. It also establishes, as a Specific Offense Characteristic, that if "the retail value of the infringing items exceeded \$2,000," then the guideline level is increased by the corresponding number of levels from the table in U.S.S.G. § 2F1.1 (Fraud and Deceit). The Commentary further makes clear that the term "infringing items," as used above, "means the items that violate the copyright or trademark laws (not the legitimate items that are infringed upon)."

The Sentencing Guidelines unequivocally require consideration of "the retail value of the infringing items." It is not entirely clear, however, what "retail value" means in the trademark or copyright context. "Retail value" is commonly associated with the sale of legitimate items because the price of such items normally relates to the manufacturer's suggested retail price when the items are generally distributed through conventional retail channels. By comparison, infringing items have no equivalent "retail value" unless one considers, for example, their prices on the black or "thieves'" market. The background commentary does little to clarify this issue, noting only that "the enhancement is based on the value of the infringing items, which will generally exceed the loss or gain due to the offense." In fact, however, such an accounting will not adequately reflect the "loss" attributable to the offense, because "loss" under the guidelines reflects only the loss to public consumers, and not the potentially greater losses to sellers of legitimate, non-infringing goods.⁸⁸

⁸⁷ Effective November 1, 1993, the previous § 2B5.4 (Criminal Infringement of Trademark) was deleted in its entirety and consolidated with § 2B5.3, which now controls criminal infringement of a copyright or trademark. See Sentencing Guidelines Appendix C, amendments 481 and 482.

⁸⁸ The narrow view of "loss" adopted in this portion of the Guidelines fails to recognize the potentially more
(continued...)

As discussed above, see "*Sentencing Guidelines*," *supra* p. 37, courts in several copyright infringement cases have, at least implicitly, recognized these difficulties, and employed various theories to achieve equitable results. In *United States v. Kim*, 963 F.2d 65, 68 (5th Cir. 1992), the court specifically held that the phrase "retail value of the infringing items" refers to the retail value of the counterfeit merchandise.⁸⁹ However, the *Kim* court found that the district court's sentencing based on the retail value of the genuine merchandise was not clearly erroneous only because the defendant failed to introduce evidence concerning the retail value of the infringing items. *Id.*

The *Kim* court disagreed with the Second Circuit's decision in *United States v. Larracuente*, 952 F.2d 672, 674 (2d Cir. 1992), noting that the Second Circuit approved using the retail value for genuine merchandise to determine the increase in the defendant's offense level under U.S.S.G. § 2B5.3. *Kim*, 963 F.2d at 69. The court in *Larracuente* found that because "unauthorized copies [of bootleg tapes] are prepared with sufficient quality to permit their distribution through normal retail outlets, the value of the infringing items is their normal retail price." *Larracuente*, 953 F.2d at 674. The Second Circuit expressly noted, however, "[w]e would have a different question if the infringing items were of obviously inferior quality and were for that reason distributed to consumers who pay far less than the retail price for authentic items." *Id.* at 675.

Similarly, the court in *United States v. Sung*, 51 F.3d 92, 96 (7th Cir. 1995), held that the "retail value of the infringing products" is the retail value of seized, unsold goods if the government can establish with "'reasonable certainty,' subject to a deduction of 3 levels under U.S.S.G. § 2X1.1(b)(1)" that the defendant "was about to complete all [necessary] acts but [for] apprehension." *Id.* (citation omitted). The Seventh Circuit remanded the case to the district court to determine whether the sentencing calculations should include the retail value of the defendant's purchase of 240,000 boxes of infringing hair spray, which were seized from him by the government.

(...continued)

sizeable losses suffered by legitimate sellers in the form of lost retail sales. Note that guidelines for similar offenses adopt a broader concept of "loss." See e.g., U.S.S.G. § 2B1.1 (Larceny, Embezzlement, and Other Forms of Theft) (Commentary, Application Note 2) ("Where the market value is difficult to ascertain or inadequate to measure the harm to the victim, the court may measure loss in some other way, such as reasonable replacement cost to the victim."). See also *United States v. Ciansciewski*, 894 F.2d 74 (3d Cir. 1990) (cost to victim of stolen check is full amount of check, not price at which stolen check is resold); *United States v. Wilson*, 900 F.2d 1350 (9th Cir. 1990) (sentencing court acted reasonably when it considered victim's development cost to measure intended loss, and was not limited to strict market valuation of loss).

⁸⁹ The court in *Kim* analyzed § 2B5.4 and not § 2B5.3. However, the language in the former section was identical to the present § 2B5.3 and was consolidated into that section. Thus, the *Kim* decision seems equally applicable today.

3. Forfeiture

a. *Criminal*

The forfeiture provision, contained at 18 U.S.C. § 2320(b), resembles a civil, rather than a criminal provision. It provides that "[u]pon a determination by a preponderance of the evidence that any articles in the possession of a defendant in a prosecution under this section bear counterfeit marks, the United States may obtain an order for the destruction of such articles." In choosing a civil-type forfeiture provision, the joint committee explained that "[e]ven if the defendant is ultimately acquitted of the criminal charge, there is no valid public policy reason to allow the defendant to retain materials that are in fact counterfeit." Joint Statement at H12077.

b. *Civil*

In addition to allowing government seizures of infringing items under a § 2320 prosecution, the Lanham Act also provides, at least to a limited extent, for ex parte seizures initiated by private trademark owners. Because the Lanham Act requires trademark owners seeking an ex parte order to give reasonable notice to the United States Attorney, 15 U.S.C. § 1116(d)(2), and because the actual seizures of the infringing goods can only be made by a federal or state law enforcement officer, 18 U.S.C. § 1116(d)(9),⁹⁰ federal prosecutors should be familiar with the civil seizure provisions.

In order to obtain an ex parte seizure order, an applicant must establish, inter alia, that the applicant is:

likely to succeed in showing that the person against whom seizure would be ordered used a counterfeit mark in connection with the sale, offering for sale, or distribution of goods or services.

15 U.S.C. § 1116(d)(4)(B)(iii).⁹¹

⁹⁰ On July 2, 1996, Congress amended this subsection to permit any "state or local law enforcement officer" to carry out a seizure of infringing items. Anticounterfeiting Consumer Protection Act of 1996, Pub. L. No. 104-153, 110 Stat. 1386 (1996). Prior to this, only "United States Marshals" were specifically authorized to carry out a seizure order. The court also has the discretion to appoint a security agency to carry out the seizure, as well as to allow the plaintiff's attorney to accompany and assist the law enforcement officials executing the order. 15 U.S.C. § 1116(d)(9).

⁹¹ Under this provision, ex parte seizures can only be made of "counterfeit goods," which excludes "parallel imports," "gray goods" and "production overruns." (For a discussion of these terms see "Lanham Act defenses," supra (continued...))

The plaintiff must also show that the defendant "would destroy, move, hide, or otherwise make" the counterfeit goods "inaccessible to the court" if notice were given. 15 U.S.C. § 1116(d)(4)(b)(vii). Thus, courts should not order a seizure against a "reputable merchant," absent unusual circumstances.⁹² In addition, the plaintiff must establish that the counterfeit goods "will be located at the place identified in the application." 15 U.S.C. § 1116(d)(4)(b)(v).

Further, the applicant must make the traditional showings that he or she would suffer irreparable injury if the goods were not seized, 15 U.S.C. § 1116(d)(4)(B)(iv), and that the balance of hardships tips in his or her favor. 15 U.S.C. § 1116(d)(4)(B)(vi).

In addition to the substantive requirements, certain procedural requirements must be met. These include posting a bond adequate to pay for damages incurred by any person "as a result of a wrongful seizure," 15 U.S.C. § 1116(d)(4)(A), an assurance against publicity, and a requirement for a prompt post-seizure hearing. Of particular importance for federal prosecutors is the requirement that the United States Attorneys are to be given "such notice as is reasonable under the circumstances" of the impending *ex parte* seizure. 15 U.S.C. § 1116(d)(2). Moreover, that subsection also provides that the United States Attorney "may participate in the proceedings arising under [an *ex parte* seizure] application if such proceedings may affect evidence of an offense against the United States. The court may deny such application if the court determines that the public interest in a potential prosecution so requires."

D. CONTRASTING THE TRADEMARK AND THE COPYRIGHT ACT

The trademark counterfeiting statute may apply in some cases where the criminal copyright statute does not. For example, unlike the criminal copyright scheme, the trademark counterfeiting statute does not require that a minimum number of copies be reproduced or distributed to constitute a felony. Rather, the law reaches all trafficking in counterfeit goods,

(...continued)

p. 59). Thus, the scope of this provision equals that of 18 U.S.C. § 2320.

⁹² According to the joint statement:

A reputable businessperson would not be likely to conceal or destroy evidence when notified of a pending lawsuit, and the issuance of an *ex parte* seizure order against such a person would therefore be wholly inappropriate, absent the unusual circumstances just mentioned. Rather, the sponsors believe that *ex parte* seizures are a necessary tool to thwart the bad faith efforts of fly by night defendants to evade the jurisdiction of the court.

Joint Statement at H12081.

"including trafficking that is discovered in its incipiency, such as before the counterfeit merchandise has left the factory."⁹³ Joint Statement at H12079.

The trademark statute also can be used in certain cases where proving the Copyright Act's element of "commercial advantage or private financial gain" may be difficult. The definition of trafficking expressly includes instances where an individual makes or obtains control of a counterfeit item with an intent to "transport, transfer, or otherwise dispose of to another, as consideration for anything of value." 18 U.S.C. § 2320(d)(2). At least one court has read the "anything of value" requirement broadly to include goods offered by a defendant in exchange for a "good will" arrangement to provide a continuing supply of other counterfeit goods. "Such 'good will' can be considered a thing of value in the form of an intangible asset." United States v. Koehler, 24 F.3d 867, 871 (6th Cir.1994)(citing Newark Morning Leger Co. v. United States, 507 U.S. 546, 556 (1993)).

Importantly, while the criminal copyright statute is subject to a three-year statute of limitations, 17 U.S.C. § 507(a), prosecutions for trademark counterfeiting under 18 U.S.C. § 2320 are covered by the traditional five-year limitations period. See 18 U.S.C. § 3282.

E. CHARGING BOTH CRIMINAL COPYRIGHT AND TRADEMARK VIOLATIONS

Charging both copyright and trademark violations arising from the same act or acts does not violate the Double Jeopardy Clause of the Fifth Amendment of the Constitution because "each offense contains an element not contained in the other." United States v. Dixon, 509 U.S. 688, 698 (1993) (citing Blockburger v. United States, 284 U.S. 299, 304 (1932)). Accordingly, inconsistent verdicts from a trial involving charges of copyright infringement and trademark counterfeiting should not jeopardize a successful conviction. See United States v. Sheng, 26 F.3d 135 (9th Cir. 1994). Similarly, a jury's inability to reach a verdict on an accompanying conspiracy count does not necessarily affect a finding of guilt on the substantive count or counts. United States v. Steele, 785 F.2d 743, 750 (9th Cir. 1986)(criminal copyright case).

It may be appropriate to bring trademark counterfeiting charges in criminal copyright infringement cases. Often, for example, manufacturers or vendors of infringing items may illegally attempt to reproduce the packaging for genuine copyrighted works. This packaging often carries counterfeit trademarks, which will support charges under the trademark counterfeiting statute. In several early cases involving sound recordings and motion pictures, pirates were charged under 18

⁹³ It should also be noted that the trademark counterfeiting seizure provision requires that civil litigants seeking to obtain ex parte seizure of infringing goods notify the U.S. Attorney of such intentions; no such requirement is placed on litigants seeking ex parte seizure in copyright cases.

U.S.C. § 2320 with illegitimately reproducing recording labels, manuals, or packaging, in addition to being charged with copyright violations for reproducing the underlying work on audio or videotape.⁹⁴ Similarly, it is not uncommon for software counterfeiters to reproduce not only the underlying code (supporting charges for copyright infringement), but also to reproduce the instruction manuals and packaging traditionally offered by a legitimate seller of these products. Reproducing the text of an instruction manual can give rise to an another charge of copyright infringement, as well as an additional charge under § 2320⁹⁵ if the infringing copy bears a registered trademark.

It may be possible to charge a § 2320 violation even in cases where the defendant did not attempt to copy genuine packaging, but did knowingly reproduce the counterfeit mark in the course of reproducing the product itself. "Once a product is put into commerce, any confusion, mistake, or deception occurring at some future time is sufficient to establish liability for trademark infringement." Sega Enters. Ltd. v. MAPHIA, 1996 WL 734409 (N.D. Ca. Dec. 18, 1996). In Maphia, the court granted plaintiff's motion for summary judgment where the defendant operated a BBS that facilitated the distribution of plaintiff's computer games. When the downloaded game was played, the game began with a screen showing plaintiff's federally registered trademark. The court rejected defendant's claim that plaintiff's trademark was being used merely "as a file identifier" and such use does not violate the Lanham Act. The court stated that the use of plaintiff's trademark "creates the likelihood of confusion as to whether Sega endorsed or sponsored the games made available on defendant's BBS." "Accordingly. . . . [defendant's] use of Sega's trademark on virtually identical Sega game programs constitutes counterfeiting." Id. at 16.

⁹⁴ Note that in such cases, prosecutors might also consider the propriety of charging violations of 18 U.S.C. § 2318. See "Trafficking in Counterfeit Labels, 18 U.S.C. § 2318," supra p. 42.

⁹⁵ Literally thousands of trade and service marks have been registered, relatively recently, by the computer industry. A very small sampling of marks contained on the principal register appears below:

"Apple," "Macintosh," "Powerbook," "Newton,"
"IBM," "Think pad," "Prodigy,"
"Lotus," "Smartsuite," "Symphony," "123,"
"Microsoft," "Bookshelf," "Powerpoint,"
"Novell" "Netware,"
"Wordperfect," "Pageperfect."

V. PROSECUTION OF THEFT OF TRADE SECRETS

A. INTRODUCTION

Unlike copyright and trademark law, which trace their roots to well-established British common law principles, the law of trade secrets, while not without a common law basis, is relatively recent and rapidly evolving. In fact, it is still not universally accepted that a trade secret is a type of property. Moreover, with one minor exception,⁹⁶ until very recently there was no federal statute that explicitly criminalized the theft of trade secrets. Federal courts, however, under limited circumstances, did uphold convictions for the interstate transportation of stolen trade secrets or proprietary economic information under 18 U.S.C. § 2314, or for the disclosure of information in violation of a confidential or fiduciary relationship under 18 U.S.C. §§ 1341 or 1343.

Because federal prosecutors have had trouble "shoe-horning" the theft of trade secrets into the above statutes and because intellectual property plays an increasingly important role in the well-being of the American economy, Congress enacted the Economic Espionage Act of 1996, effective October 11, 1996.⁹⁷ Pub.L. 104-294, 110 Stat. 3489. In general, it criminalizes the theft of trade secrets.⁹⁸

⁹⁶ 18 U.S.C. § 1905 provides, *inter alia*, for misdemeanor sanctions for the unauthorized disclosure of government information, including trade secrets, by a government employee.

⁹⁷ As noted by Senator Arlen Specter, a co-sponsor of the Economic Espionage Act:

In an increasing complex and competitive economic world, intellectual property forms a critical component of our economy. As traditional industries shift to low-wage producers in developing countries, our economic edge depends to an ever-increasing degree on the ability of our business and inventors to stay one step ahead of those in other countries. And American business and inventors have been extremely successful and creative in developing intellectual property and trade secrets. America leads the nations of the world in developing new products and new technologies. Millions of jobs depend on the continuation of the productive minds of Americans, both native born and immigrants who find the freedom here to try new ideas and add to our economic strength.

Inventing new and better technologies, production methods, and the like, can be expensive. American companies and the U.S. Government spend millions on research and development. The benefits reaped from these expenditures can easily come to nothing, however, if a competitor can simply steal the trade secret without expending the development costs. While prices may be reduced, ultimately the incentives for new invention disappear, along with jobs, capital investment, and everything else that keeps the economy strong.

142 Cong. Rec. S12201, 12209 (daily ed. Oct. 2, 1996) (statements of Sen. Specter).

⁹⁸ For additional discussion of the Economic Espionage Act of 1996 see James H.A. Pooley, Mark A. Lemley, and Peter J. Toren, Understanding the Economic Espionage Act of 1996, 5 Tex. Int. Prop. L.J. 177 (Winter 1997).

B. THE ECONOMIC ESPIONAGE ACT OF 1996

1. Overview of the Statute

The Economic Espionage Act of 1996 ("EEA") contains two separate provisions that criminalize the theft or misappropriation of trade secrets. The first provision, codified at 18 U.S.C. § 1831, is directed towards foreign economic espionage and requires that the theft of the trade secret be done to benefit a foreign government, instrumentality, or agent.⁹⁹ In contrast, the second provision makes criminal the more common commercial theft of trade secrets, regardless of who benefits. 18 U.S.C. § 1832.¹⁰⁰ Reflecting the more serious nature of economic espionage, a defendant convicted of violating § 1831 can be imprisoned for up to 15 years and

⁹⁹ Section 1831 provides:

(a) IN GENERAL.—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (4), and one or more of such person do any act to effect the object of the conspiracy, is guilty of a felony.

¹⁰⁰ Section 1832 provides:

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, is

guilty of a felony.

fined \$500,000 or both, 18 U.S.C. § 1831(a)(5), whereas a defendant convicted for theft of trade secrets under § 1832 can be imprisoned for up to 10 years and fined \$500,000 or both. 18 U.S.C. 1832(a)(5).

There are a number of important features to the EEA, including a provision for the criminal forfeiture of any property or proceeds derived from a violation of the EEA. 18 U.S.C. § 1834. The EEA also permits the Attorney General to institute civil enforcement actions and obtain appropriate injunctive relief for violations. 18 U.S.C. § 1836. Further, because of the recognized difficulty of maintaining the secrecy of a trade secret during litigation, the EEA requires that courts take such actions as necessary to preserve the confidentiality of the trade secret. 18 U.S.C. § 1835. The EEA also covers conduct occurring outside the United States where the offender is a citizen or permanent resident alien of the United States, or an act in furtherance of the offense was committed in the United States. 18 U.S.C. § 1837. Finally, all prosecutions brought under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division.¹⁰¹

2. Elements common to §§ 1831 and 1832

The EEA contains two separate sections that criminalize the theft of trade secrets. Under each section, the government must prove beyond a reasonable doubt that (1) the defendant stole, or without authorization of the owner, obtained, destroyed or conveyed information; (2) the defendant knew this information was proprietary; and (3) the information was in fact a trade secret. To establish a violation of the economic espionage provision, the government must also prove that the defendant knew the offense would benefit or was intended to benefit a foreign government, foreign instrumentality, or foreign agent.

If the government cannot establish that the defendant acted with the intent to benefit a foreign entity, the government can still establish a violation of the EEA under 18 U.S.C. § 1832 if it can establish, in addition to the first three elements described above, that: (4) the defendant intended to convert the trade secret to the economic benefit of anyone other than the owner; (5) the defendant knew or intended that the owner of the trade secret would be injured; and (6) the trade secret was related to or was included in a product that was produced or placed in interstate or foreign commerce.

Both sections also explicitly criminalize attempts and conspiracies to engage in economic espionage and steal trade secrets. 18 U.S.C. §§ 1831(a)(4), (a)(5) and 1832(a)(4), (a)(5).

¹⁰¹ Prior to the passage of the EEA, the Attorney General assured Congress in writing that the Department of Justice will require that all prosecutions brought under the EEA be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. See "Department of Justice Oversight," *infra* p. 85.

Additionally, both sections make criminal the knowing receipt, purchase or possession of a stolen trade secret. 18 U.S.C. §§ 1831(a)(3), 1832(a)(3).

a. *Misappropriation*

The initial element of a criminal prosecution under either § 1831 or § 1832 is that the defendant obtained, destroyed or conveyed information without the authorization of the owner. The type of acts which are prohibited are broadly defined and include traditional instances of theft, i.e., where the object of the crime is physically removed from the owners possession, 18 U.S.C. §§ 1831(a)(1), 1832(a)(2). However, less traditional methods of misappropriation and destruction are also included within the terms of the EEA. Under 18 U.S.C. §§ 1831(a)(2) and 1832(a)(2), the prohibited acts include copying, duplicating, sketching, drawing, photographing, replicating, transmitting, delivering, sending, mailing, communicating, or conveying. With these methods the original property never leaves the custody or control of the owner, but the unauthorized duplication or misappropriation may effectively destroy the value of what is left with the rightful owner. Through copying, information can be stolen without asportation, and the original object remains intact. It was the intent of Congress "to ensure that the misappropriation of intangible information is prohibited in the same way that the theft of physical items are protected." S.Rep. No. 359, 104th Cong., 2d Sess. 16 (1996).

The government must prove that the defendant acted "without authorization" from the owner. This refers to whether the defendant had the consent of the owner to obtain, destroy or convey the trade secret. According to the legislative history, "authorization is the permission, approval, consent or sanction of the owner" to obtain, destroy or convey the trade secret. 142 Cong. Rec. S12202, S12212 (daily ed. Oct. 2, 1996). Thus, for example, where an employee has authorization from his employer to obtain a trade secret during the regular course of employment, he can still violate the EEA if he "conveys" it to a competitor without his employer's permission.

b. *Knowledge*

The first *mens rea* element that the government must prove is that the defendant's misappropriation was done "knowingly." Thus, it must show that the defendant knew or had a firm belief that information he or she was taking was proprietary. 142 Cong. Rec. at S12213 (daily ed. Oct. 2, 1996). Generally, under criminal statutes covering the theft of tangible property, the government must prove that the thief knew that the object he stole was property that he had no lawful right to convert it for his personal use. Applying this same principle to this statute, in order for the defendant to be convicted, the government must establish that the defendant was aware or substantially certain that he was misappropriating a trade secret. Thus, a person who

takes a trade secret because of ignorance, mistake or accident cannot be prosecuted under the EEA. The legislative history goes on to suggest that:

[t]his requirement should not prove to be a great barrier to legitimate and warranted prosecutions. Most companies go to considerable pains to protect their trade secrets. Documents are marked proprietary; security measures put in place; and employees often sign confidentiality agreements to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items are protected.

Id.

c. *Trade secret*

The definition of the term "trade secret" in the EEA is very broad. It includes, generally, all types of information, however stored or maintained, which the owner has taken reasonable measures to keep secret and which has independent economic value.¹⁰² It is broader than the definition of "trade secret" in the Uniform Trade Secrets Act¹⁰³ in a number of respects, but prior case law should be instructive in illuminating the EEA's definition of a trade secret.

¹⁰² 18 U.S.C. § 1839 defines a "trade secret" as:

all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if-

(a) the owner thereof has taken reasonable measures to keep such information secret; and

(b) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

¹⁰³ Section 1(4) of the Uniform Trade Secrets Act provides:

(4) "Trade secret" means information, including a formula pattern, compilation, program, device, method technique, or process that

(I) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Unlike patents, which must be both novel and a step beyond "prior art," trade secrets must be only "minimally novel." Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974). In other words, a trade secret must contain some element that is not known and sets it apart from what is generally known. According to the legislative history of the EEA, "[w]hile we do not strictly impose a novelty or inventiveness requirement in order for material to be considered a trade secret, looking at the novelty or uniqueness of a piece of information or knowledge should inform courts in determining whether something is a matter of general knowledge, skill or experience." 142 Cong. Rec. S12201, S12212 (daily ed. Oct. 2, 1996).

The sine qua non of information constituting a trade secret is that it is not publicly known. Whether the information was secret before it was obtained by the defendant is a question of fact. The government often has the difficult burden of proving a negative, i.e., that the information was not generally available to the public. In this regard, prosecutors should make sure that the information had not been publicly disclosed through, for example, technical journals or other publications and should determine whether the information was obvious to the victim's competitors in the industry. Often information that a company regards as its proprietary "crown jewels" is well-known in the industry and, therefore, not protected.

Every part of the information need not be completely confidential to qualify for protection as a trade secret. A trade secret can include a combination of elements that are in the public domain, if the trade secret constituted a unique, "effective, successful and valuable integration of the public domain elements." Rivendell Forest Prods. Ltd. v. Georgia-Pacific Corp., 28 F.3d 1042, 1046 (10th Cir. 1994); see also Apollo Technologies v. Centosphere Indus., 805 F. Supp. 1157, 1197 (D.N.J. 1992).

Trade secrets are also fundamentally different from other forms of property in that the owner of a trade secret must take reasonable measures under the circumstances to keep the information confidential. 18 U.S.C. § 1839(3)(A). This requirement, not imposed upon owners of other types of property,¹⁰⁴ is necessary to insure that a person cannot obtain a monopoly on ideas that are in the public domain.

The extent of the security measures taken by the owner of the trade secret need not be absolute, but must be reasonable under the circumstances, depending on the facts of the specific case. See e.g., Pioneer Hi-Bred Int'l v. Holden Found Seeds, 35 F.3d 1226, 1235 (8th Cir. 1994); Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823, 848-49 (10th Cir. 1993). "Reasonable efforts" can include advising employees of the existence of a trade secret, limiting access to the information to a "need to know basis," requiring employees to sign confidentiality agreements, MAI Sys. Corp. v. Peak Computer, 991 F.2d 511, 521 (9th Cir. 1993), and keeping secret documents under lock. 1 Roger Milgrim, Milgrim on Trade Secrets, § 1.04 at 1-126.

¹⁰⁴ For example, a defendant can be convicted for stealing a bike even if the victim failed to protect it by leaving it unlocked on his front porch.

Each trade secret owner must assess the value of the protected material and the risk of its theft in devising reasonable security measures. Under this principle, prosecutors must be able to establish that the security measures used by the victim to protect the trade secret were commensurate with the value of the trade secret. For example, prosecutors should determine the extent of the security used to protect the trade secret, including physical security, computer security, and the company's policies on sharing information with, for example, sub-contractors and licensed vendors. If investigation reveals, for example, that any low-level employee in a very large company could gain access to the information, it might not qualify as a trade secret.

Courts have held that information may remain a trade secret even if the owner discloses the information to its licensees, vendors, or third parties for limited purposes. See, e.g., Rockwell Graphic Sys., Inc. v. DEV Industries, Inc., 925 F.2d 174 (7th Cir. 1991). The owner of the trade secret must, however, take reasonable security measures when it does disclose the information, such as requiring non-disclosure agreements. Further, a trade secret can lose its protected status if it is disclosed, for example, either through legal filings (such as by the issuance of a patent), or through accidental or intentional disclosure by an employee at conferences, at trade shows, or in writings. See e.g., Apollo Technologies v. Centrosphere Indus., 805 F. Supp. 1157, 1198 (D.N.J. 1992). At least one court has held that information can lose its status as a trade secret through an anonymous posting on the Internet, even for a very limited time. Religious Technology Ctr. v. Netcom On-Line Com., 923 F. Supp. 1231 (N.D. Cal. 1995).

Finally, the trade secret must derive "independent economic value . . . from not being generally known to . . . the public." 18 U.S.C. § 1839(3)(B). Since the EEA does not require that the government prove a specific jurisdictional amount, proving this element should not be difficult.

In limited circumstances, the value of the trade secret can be established by showing what the trade secret fetched on the open market. For example, in United States v. Bottone, 365 F.2d 389 (2d Cir.), cert. denied, 385 U.S. 974 (1966), the court held that the value of stolen chemical formulae could be based on what European drug manufacturers were willing to pay. Similarly, in United States v. Greenwald, 479 F.2d 320 (6th Cir.), cert. denied, 414 U.S. 854 (1973), the Sixth Circuit held that value of the misappropriated trade secret could be established from the "viable, albeit limited" market among chemical companies for the type of formulae misappropriated and from licensing agreements or sales for the chemical formulae that were misappropriated. Id. at 322.

In those instances where the value of the trade secret cannot be established through the use of a legitimate market, courts have approved the use of a "thieves" market as a proper means of valuing stolen goods or property under a variety of federal statutes. See, e.g., United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988) (18 U.S.C. § 2314); United States v. Drebin, 557 F.2d 1316, 1328 (9th Cir. 1977) (18 U.S.C. § 2314); Churder v. United States, 387 F.2d 825, 833 (8th Cir. 1968) (18 U.S.C. § 641); United States v. Oberhardt, 887 F.2d 790, 793 (7th Cir.

1989) (18 U.S.C. § 641); United States v. Berkowitz, 619 F.2d 649, 657 (7th Cir. 1980) (18 U.S.C. § 2311).

In many situations involving the misappropriation of trade secrets, however, monetary value is not easily established, either because the trade secret is often stolen at the development stage or because the victim company has chosen not to sell or license the technology. Consequently there is no true market value, i.e., what a willing buyer would pay a willing seller in the open market. In such situations, federal courts generally have rejected a strict market valuation approach and have found that "where the goods have no readily ascertainable market value, 'any reasonable method may be employed to ascribe an equivalent monetary value. . . .'" United States v. Drebin, 557 F.2d 1316, 1331 (9th Cir. 1972) (quoting United States v. Lester, 282 F.2d 750, 755 (3rd Cir. 1960), cert. denied, 364 U.S. 937 (1961)); see also United States v. Seagraves, 265 F.2d 876, 880 (3rd Cir. 1959). These methods include consideration of the development, research and production costs. See, e.g., United States v. Wilson, 900 F.2d 1350, 1356 (9th Cir. 1990); United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988). But see Abbott v. United States, 239 F.2d 310, 313 (5th Cir. 1956) (value for the purposes of 18 U.S.C. § 2314 includes only market value.)

Although development, research and production costs may be relevant to the value of the trade secret, prosecutors should be careful in relying exclusively on this method of valuation. The true value of the information may be far more or far less than the cost of development and may depend on immeasurable attributes, such as the originality or soundness of the underlying ideas. Further, at trial, prosecutors should consider using an independent expert witness to establish the valuation of the trade secret based on alternative theories, and not rely solely on the information supplied by the victim. For example, in Stegora, 849 F.2d at 292, the court approved the government's use of an expert witness to establish that the 3M Company spent in excess of \$1,000,000 for research, development and manufacturing equipment to market the product, and that a license to produce a product using the technology described in the trade secret would cost \$150,000 per million dollars of sales.

3. Additional § 1831 Element

a. *Intent to benefit a foreign government, foreign instrumentality, or foreign agent*

The second mens rea requirement of a § 1831 violation is that the defendant intended or knew that the offense would "benefit" a "foreign government, foreign instrumentality,"¹⁰⁵ or foreign

¹⁰⁵ The term "foreign instrumentality" means:

(continued...)

agent."¹⁰⁶ Thus, the government must show that the defendant knew or had a firm belief that misappropriation would benefit a foreign entity. When this "entity" is not, per se, a government entity (e.g., a business), there must be evidence of foreign government sponsorship or "coordinated intelligence activity." 142 Cong. Rec. S12201, S12212 (daily ed. Oct. 2, 1996)

The legislative history of the EEA indicates that "benefit" is to be interpreted broadly and is not limited to an economic benefit, but includes a "reputational, strategic, or tactical benefit." H.R. Rep. No. 788, 104th Cong., 2d Sess. (1996).

The requirement that the benefit accrue to a foreign government, instrumentality or agent should be very carefully analyzed by government prosecutors. In order to establish that the defendant intended to benefit a "foreign instrumentality" the government must show that the entity was "substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government." 18 U.S.C. § 1839(1). The EEA does not define "substantially," but its use suggests that the prosecution does not have to prove complete ownership, control, sponsorship, command, management or domination. The legislative history states:

substantial in this context, means material or significant, not technical or tenuous. We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns 10 percent of a company exempt it from scrutiny. Rather the pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.

142 Cong. Rec. S12201, S12212 (daily ed. Oct. 2, 1996).

Thus, § 1831 does not apply where a foreign corporation misappropriates the trade secret and there is no evidence of sponsorship or "coordinated intelligence activity" by a foreign government. Id. at S12213. In such an instance, however, the foreign corporation could still be properly charged under § 1832.

¹⁰⁵(...continued)

any agency, bureau, component, institution, association, or any legal, commercial, or business organization, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.

18 U.S.C. § 1839(1).

¹⁰⁶ The term "foreign agent" means:

any officer, employee, proxy, servant, delegate, or representative of a foreign government.

18 U.S.C. § 1839(2).

4. Additional section 1832 elements

a. *Economic benefit to a third party*

Under § 1832 the government must prove that the act of misappropriating the trade secret was intended for the economic benefit of a person other than the rightful owner (which can be the defendant or some other person or entity). This differs from § 1831 where foreign government activity is required, and the benefits may be non-economic. Therefore, a person who misappropriates a trade secret but who does not intend for anyone to gain economically from the theft cannot be prosecuted under § 1832.

b. *Intent to injure the owner of the trade secret*

Beyond demonstrating that the defendant both knew the information taken was proprietary and intended that the misappropriation economically benefit someone other than the rightful owner, the government in a § 1832 case also must prove a third mens rea element: that the defendant intended to "injure" the owner of the trade secret. According to the legislative history of the EEA, this provision "does not require the government to prove malice or evil intent, but merely that the actor knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner." H.R. Rep. No. 788, 104th Cong., 2d Sess. 1996.

Under this standard, it is not entirely clear what the government has to prove, if anything, in addition to proving that the defendant intended to misappropriate the trade secret to benefit another. By definition, in order for a trade secret to have value, it must confer a commercial advantage to the owner. Further, the value is dependent on keeping the information a secret. Once the information is disclosed to another for the recipient's benefit, the trade secret loses its value. In this context, each time a defendant discloses a trade secret, the owner is injured to the extent that the trade secret has lost at least a portion of its value.

c. *Interstate or foreign commerce*

This element requires the government to prove that the trade secret was "related to or included in a product that is produced for or placed in interstate or foreign commerce." 18 U.S.C. § 1832. In cases where the trade secret is related to a product actually being manufactured and sold, this element would be easily established by evidence of interstate sales. However, where the trade secret relates to a product in research and development, proof would be much more difficult. It is possible for a defendant to argue that products still in the research

and development stage are not yet being "produced for interstate commerce" because such items are not yet being "produced" for sale. If this argument prevails, much of the protection of the EEA would be lost, because a trade secret is often most valuable during the development phase. Once the product embodying the trade secret is released to the public, the value of the trade secret is often lost because the product can be examined and the trade secret obtained, for example, through reverse engineering.

There is no evidence that Congress intended to create such a large exception to the trade secrets accorded protection under the EEA. Therefore, in cases in which the trade secret is related to a product still being developed but will ultimately be sold in interstate commerce, prosecutors should establish this fact, and argue that it sufficiently meets this element.

5. Defenses

a. *Parallel development*

The owner of a trade secret, unlike the holder of a patent, does not have an absolute monopoly on the information or data that comprises the trade secret. Other companies and individuals have the right to discover the elements of a trade secret through their own research and hard work. As the Supreme Court stated in Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 490-91 (1974):

If something is to be discovered at all, very likely it will be discovered by more than one person. . . . Even were an inventor to keep his discovery completely to himself, something that neither the patent nor trade secret laws forbid, there is a high probability that it will be soon independently developed. If the invention, though still a trade secret, is put into public use, the competition is alerted to the existence of the inventor's solution to the problem and may be encouraged to make an extra effort to independently find the solution thus known to be possible.

Thus, it is a defense if the defendant demonstrates that he independently developed the trade secret.

b. *Reverse engineering*

Similarly, a person can legally discover the elements of a trade secret by "reverse engineering," the practice of taking something apart to determine how it was made or

manufactured. See, e.g., Kewanee Oil Co., 416 U.S. at 476 (the law does not protect the owner of a trade secret from "discovery by fair and honest means, such as independent invention, accidental disclosure, or by so-called reverse engineering."). The EEA does not expressly address when reverse engineering would be a valid defense; however, the legislative history suggests that "the important thing is to focus on whether the accused has committed one of the prohibited acts of this statute rather than whether he or she has reverse engineered. If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent, or this law, then that form of 'reverse engineering' should be fine." 142 Cong. Rec. S12201, S12212 (daily ed. Oct. 2, 1996).

Therefore, to avoid a successful claim by the defendant that he discovered the trade secret by reverse engineering, prosecutors should establish the means by which the defendant misappropriated the trade secret. For example, if the prosecution could show that the defendant unlawfully obtained access to the trade secret, it would refute his claim that he learned of the trade secret through reverse engineering. Further, a defendant cannot defeat a prosecution by claiming the trade secret "could have been discovered by reverse engineering." Telerate Sys. Inc. v. Caro, 689 F. Supp. 221, 232 (S.D.N.Y. 1988) ("the proper focus of inquiry is not whether an alleged trade secret can be deduced by reverse engineering but rather, whether improper means are required to access it.").

c. *General knowledge*

The EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skill or abilities. Employees, for example, who change employers or start their own companies cannot be prosecuted based on an assertion that they were exposed to a trade secret while employed, unless the government can establish that they stole or misappropriated a particular trade secret. The legislative history makes clear that "[t]he government can not prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company. Allowing such prosecutions to go forward and allowing the risk of such charges to be brought would unduly endanger legitimate and desirable economic behavior." 142 Cong. Rec. S12201, 12213 (daily ed., Oct. 2, 1996). This does not mean, however, that employees who leave a company to start their own companies or change jobs can never be prosecuted under the EEA. Where the employees stole or without authorization appropriated a trade secret from their employer, they may be prosecuted under § 1832, assuming, of course, that the other elements can also be satisfied.¹⁰⁷

¹⁰⁷ Clear evidence of theft or copying is helpful in all cases to overcome the potential problem of prosecuting the defendant's "mental recollections" and a defense that "great minds think alike."

d. *The First Amendment*

In most instances, if the government can establish that the defendant intended for the misappropriation to benefit economically a third party, he should not be able to claim successfully that the First Amendment of the Constitution protected the disclosure of the trade secret. In other words, if the defendant's motivation was pecuniary, he cannot very well argue that he disclosed the secret as a public service or to educate the public. Further, courts also have rejected a First Amendment defense if the speech itself is the very vehicle of the crime. See, e.g., *United States v. Morrison*, 844 F.2d 1057, 1068 (4th Cir.) (court rejected defendant's First Amendment defense and upheld conviction for a violation of 18 U.S.C. § 641 for stealing secret government documents, noting, "[w]e do not think that the First Amendment offers asylum . . . just because the transmittal was to a representative of the press."), *cert. denied*, 488 U.S. 908 (1988); *United States v. Rowlee*, 899 F.2d 1275 (2d Cir.), *cert. denied*, 498 U.S. 828 (1990). Additionally, in *United States v. Riggs*, 743 F. Supp 556 (N.D. Ill. 1990), the court rejected defendant's assertion that the First Amendment provides a defense to a charge under 18 U.S.C. § 2314 for the interstate transportation of stolen computer files:

In short, the court finds no support for [defendant's] argument that the criminal activities with which he is charged . . . are protected by the First Amendment. Interpreting the First Amendment as shielding [defendant] from criminal liability would open a gaping hole in criminal law; individuals could violate criminal laws with impunity simply by engaging in criminal activities which involve speech-related activity. The First Amendment does not countenance that kind of end run around criminal law.

Id. at 560-61.

Because a claim of First Amendment protection is irrelevant to defendant's illegal activities, the government should consider seeking an *in limine* order precluding the introduction of such evidence in appropriate cases.

6. *Criminal Forfeiture*

The EEA also provides that the court in imposing sentencing shall order the forfeiture of any proceeds or property derived from violations of the EEA, and may order the forfeiture of any property used to commit or to facilitate the commission of the crime. Note that the statutory language of the first subsection is mandatory and leaves the judge no discretion. 18 U.S.C. § 1834(a)(1). With regard to the latter provision, however, the court may in its discretion take into consideration "the nature, scope, and proportionality of the use of the property in the

offense." 18 U.S.C. § 1834(a)(2). The intent of that limitation is to insure that the amount and character of the forfeited property is proportionate to the harm caused by the defendant's conduct.

As a procedural matter, indictments alleging a violation of either 18 U.S.C. § 1831 or § 1832 should contain, where appropriate, a forfeiture paragraph.

7. Civil Proceedings

While the EEA does not provide for civil forfeiture proceedings, it does authorize the government to file a civil action seeking injunctive relief. 18 U.S.C. § 1836(a). Prosecutors should consider seeking injunctive relief to prevent further disclosure of the trade secret while conducting a criminal investigation or in cases in which a defendant's conduct does not warrant criminal prosecution.

8. Confidentiality

Victims of trade secret thefts are often faced with a dilemma when deciding whether to report the matter to law enforcement authorities. Generally, victims do not want the thief to go unpunished but suspect that if they report the matter, the trade secret will be publicly aired during criminal prosecution. In drafting the EEA, Congress was clearly concerned about this issue and, to encourage reporting, sought to preserve the confidentiality of a trade secret, if possible, even after the return of the indictment. The EEA provides that the court "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835.¹⁰⁸ Therefore, prosecutors are strongly encouraged to seek the entry of orders that will preserve the status of the information as a trade secret and prevent the unnecessary and harmful disclosure of such information.

Note that courts can limit the disclosure of information to the public even during the trial without necessarily violating the defendant's right to a public trial under the Sixth Amendment. While the right to a public criminal trial was incorporated into the Constitution by the Sixth Amendment, the right is not absolute and may be limited in certain circumstances. Richmond News Papers, Inc. v. Virginia, 448 U.S. 555, 599-600 (1980) (Stewart, J. concurring); see also Gannett v. Depasquale, 443 U.S. 368, 422-33 (1979) (Marshall, J., concurring in part and

¹⁰⁸ This section also provides for interlocutory appeals from a decision or a court order authorizing the disclosure of any trade secret. Id.

dissenting in part) (tracing the history of the right to a public trial and citing cases where that right has been limited); State ex rel. La Crosse Tribune v. Circuit Court, 340 N.W. 2d 460, 466-67 (Wis. 1983) (citing State ex rel. Ampco Metal, Inc. v. O'Neil, 78 N.W. 2d 921 (Wis. 1956) (both discussing inherent power of a court to limit the public nature of trials).

At least one circuit court has recognized the power of the district court to restrict, at least partially, access to that portion of the proceeding which would reveal trade secrets. In Stamcarbon, N.V. v. American Cyanamid Co., 506 F.2d 532 (2d Cir. 1974), on appeal of a criminal contempt conviction, the court held that based on a compelling claim, a district court may partially limit the public's access if the court determines that (1) a party is likely to suffer irreparable injury if access to the proceedings was not limited, and (2) protection of the party's secrets can be achieved "with minimal disruption of the criminal proceedings." Id. at 540.

Prosecutors should therefore seek to limit the public disclosure of the trade secret during the trial by, for example, requesting that the court limit public access during the testimony of an expert witness who is describing the details of the trade secret. The release of the transcripts must be similarly limited.

9. Extraterritoriality

In order to rebut the general presumption against the extraterritoriality of U.S. criminal laws, Congress made clear that the EEA is meant to apply to specified conduct occurring outside the United States. To ensure that there is some nexus, the EEA applies to conduct occurring outside the United States if: (1) the offender is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States. 18 U.S.C. § 1837.

10. Statutory Penalties

A defendant convicted for violating § 1831 can be imprisoned for up to 15 years and fined \$500,000 or both. 18 U.S.C. § 1831(a)(5). Corporations and other organizations can be fined up to \$10,000,000. 18 U.S.C. § 1831(b). A defendant convicted for violating § 1832 can be imprisoned for up to 10 years and fined \$500,000. 18 U.S.C. § 1832(a)(5). Corporations and other entities can be fined not more than \$5,000,000 for violating that provision.

11. Department of Justice Oversight

Prior to the passage of the EEA, the Attorney General assured Congress in writing that for a period of five years, the Department of Justice will require that all prosecutions brought under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division.¹⁰⁹

C. OTHER POSSIBLE CHARGES

1. Introduction

Prior to the enactment of the EEA, with one minor exception,¹¹⁰ there was no federal statute that specifically protected trade secrets. Case law recognized, however, that the theft of

¹⁰⁹ The letter states in full:

October 1, 1996

Dear Chairman Hatch:

Thank you for your support of the Economic Espionage Act of 1996 ("Act"). The need for this law cannot be understated as it will close significant gaps in federal law, thereby protecting proprietary economic information and the health and competitiveness of the American economy.

The Department shares your concerns that the legislation be implemented in accordance with the intent of Congress and therefore will require, for a period of five years after implementation of the Act, that the United States may not file a charge under Chapter 90, or use a violation of Chapter 90 as a predicate offense under any other law, without the personal approval of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division (or the Acting official in each of these positions if a position is filled by an acting official). This requirement will be implemented by published regulation.

Violations of such regulations will be appropriately sanctionable. Any such violations will be reported by the Attorney General to the Senate and House Judiciary Committees.

Once again, thank you for your leadership in this critical area.

Sincerely,

Janet Reno

¹¹⁰ 18 U.S.C. § 1905.

trade secrets and proprietary information could violate a number of federal criminal statutes that generally prohibit the misappropriation and interstate transportation of property or goods, 18 U.S.C. § 2314, the disclosure of information in violation of a confidential or fiduciary relationship, 18 U.S.C. §§ 1341, 1343, or unlawfully accessing a protected computer, 18 U.S.C. § 1030(a)(4).

Although the applicability of these statutes to thefts of trade secrets is limited, prosecutors should, where appropriate, bring charges under both the EEA, §§ 1831 and 1832, and under one or more of these other statutes.¹¹¹

2. 18 U.S.C. § 2314

a. *Elements*

The Interstate Transportation of Stolen Property Act ("ITSP") imposes criminal liability on:

Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of \$5,000 or more, knowing the same to have been stolen, converted or taken by fraud.

Thus, in order to convict under this section, the government must prove beyond a reasonable doubt that:

- (1) the defendant unlawfully transported or caused to be transported in interstate or foreign commerce goods, wares, or merchandise;
- (2) the goods, wares, or merchandise were stolen, converted, or taken by fraud;
- (3) the goods, wares, or merchandise have a value of \$5,000 or more; and
- (4) the defendant knew the same to be stolen, converted, or taken by fraud.

See U.S.A.M. 9-61.260 - 9.61.261(A-D).

¹¹¹ Charging both a violation of the Economic Espionage Act and another statute such as Interstate Transportation of Stolen Property or Wire Fraud arising from the same act or acts does not violate the Double Jeopardy Clause of the Fifth Amendment of the Constitution because "each offense contains an element not contained in the other." United States v. Dixon, 509 U.S. 688, 690 (1993) (citing Blockburger v. United States, 284 U.S. 299, 304 (1932)).

(1) Transportation in interstate commerce

The purpose of § 2314 is to permit the federal government to come to the aid of the states "in punishing criminals whose offenses are complete under state law, but who utilize the channels of interstate commerce to make a successful getaway, and thus make the state's detecting and punitive processes impotent." United States v. Sheridan, 329 U.S. 379, 384 (1946). A prosecutor should prove this element in the same manner as with any other stolen goods, wares or other merchandise, i.e., by establishing that the good containing the trade secret was transported across state lines.

(2) Goods, wares, and merchandise

Section 2314 criminalizes the interstate transportation of stolen "goods, wares, or merchandise." However, the statute does not define these terms. Courts are divided on whether and under what circumstances intangible property such as trade secrets constitutes "goods, wares or merchandise." The defendant in United States v. Brown, 925 F.2d 1301 (10th Cir. 1991), was indicted for violating § 2314 by transporting the source code of a computer program from Georgia to New Mexico. Brown moved to dismiss the indictment arguing the government failed to allege that he transferred in interstate commerce "physical goods, wares [or] merchandise" within the meaning of § 2314. *Id.* at 1303. At an evidentiary hearing on this issue, the government admitted it could not prove either that the defendant copied the source code onto the company's diskettes or that the defendant had in his possession any tangible property belonging to the company. *Id.*

The Brown court, citing United States v. Dowling, 473 U.S. 207 (1985), dismissed the indictment.¹¹² It held that "[p]urely intellectual property," such as the source code appropriated

¹¹² In Dowling, the defendant was convicted of violating § 2314 following his interstate distribution of bootleg Elvis Presley records. The Supreme Court reversed the conviction, holding that Congress did not intend that § 2314 function as a criminalization of copyright infringement. 473 U.S. at 216-18. The Court noted that its decision did not address a situation in which the initial procurement was accomplished by theft or fraud, and acknowledged that the courts have never required that the items stolen and transported remain in entirely unaltered form. The Court emphasized, however, that:

[T]hese cases and others prosecuted under § 2314 have always involved physical 'goods, wares [or] merchandise' that have themselves been 'stolen, converted or taken by fraud.' This basic element comports with the common-sense meaning of the statutory language: by requiring that the 'goods, wares [or] merchandise' be 'the same' as those 'stolen, converted or taken by fraud,' the provision seems clearly to contemplate a physical identity between the items unlawfully obtained and those eventually transported, and hence some prior physical taking of the subject goods.

(continued...)

by the defendant, is not the type of property covered by § 2314: "It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible" and thus "cannot constitute goods, wares, merchandise which have been stolen, converted or taken within the meaning of § 2314 or 2315." 925 F.2d at 1307-08.¹¹³

The court in United States v. Bottone, 365 F.2d 389 (2d Cir.), cert. denied, 385 U.S. 974 (1966), which pre-dates Dowling, reached the opposite result. The defendants in Bottone removed papers describing manufacturing processes from their place of employment and made copies outside the office. They returned the originals and then transported the copies in interstate commerce. In upholding defendants' convictions under § 2314, Judge Friendly stated:

when the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial. It would offend common sense to hold that these defendants fall outside the statute simply because, in efforts to avoid detection, their confederates were at pains to restore the original papers to [their employer] and transport only copies or notes, although an oversight would have brought them within it

365 F.2d at 394.

Similarly, in United States v. Riggs, 739 F. Supp. 414, 420 (N.D. Ill. 1990), the court rejected the defendant's "disingenuous" argument that he merely transferred electronic impulses (albeit impulses containing computerized text files belonging to Bell South) across state lines:

[i]t is well-settled that when proprietary business information is affixed to some tangible medium, such as a piece of paper, it constitutes 'goods, wares, or merchandise' within the meaning of § 2314. . . . Therefore, in the instant case, if the information in [the computerized] text file had been affixed to a floppy disk, or printed out on a computer printer, then [defendant's] transfer of that information across state lines would clearly constitute the transfer of 'goods, wares, or merchandise' within the meaning of § 2314. This court sees no reason to hold differently simply because [defendant] stored the information inside computers instead of printing it out on paper. In either case, the information is in a transferrable, accessible, even salable form.

(...continued)
473 U.S. at 216.

¹¹³ The Brown court did distinguish a situation in which the defendant illegally appropriates a tangible item containing an intangible component, such as a chemical formula written on a stolen piece of paper. The court suggested that such an appropriation would violate § 2314, even where the value of the paper itself is insignificant and the overall value is almost wholly derived from the intangible component. 925 F.2d at 1307-08, n.14, citing United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988).

Id. at 421.¹¹⁴

While courts are split on whether an intangible trade secret constitutes "goods, wares or merchandise" for the purposes of § 2314,¹¹⁵ courts have uniformly held that transporting stolen trade secrets within a stolen tangible medium -- for example, company paper or computer diskettes -- is a violation of 18 U.S.C. § 2314. United States v. Lyons, 992 F.2d 1029, 1033 (10th Cir. 1993) ("The fact that the [defendant] stole the software in conjunction with the theft of tangible hardware distinguishes this case from Brown. Brown recognizes that the theft of intangible intellectual property in conjunction with the theft of tangible property falls within the ambit of § 2314."); United States v. Lester, 282 F.2d 750 (3d Cir.) (originals and copies of geophysical maps made by defendants on the victim's own copying equipment with the victim's supplies), cert. denied, 364 U.S. 937 (1961); United States v. Seagraves, 265 F.2d 876 (3d Cir. 1959) (same facts as Lester); United States v. Greenwald, 479 F.2d 320 (6th Cir.) (original documents containing trade secrets about fire retardation processes), cert. denied 414 U.S. 854 (1973); Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967) (state conviction for theft of 59 copies of a computer program was supported by similar federal court rulings under § 2314, citing Seagraves).

(3) Goods must have a value of \$5,000 or more

In order to fall within the scope of 18 U.S.C. § 2314, the misappropriated "goods, wares, or merchandise" must have a minimum "value" of \$5,000. The government can satisfy this burden by showing that the value of the trade secret itself was worth \$5,000 or more. See, e.g., United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988); United States v. Greenwald, 479 F.2d 320 (6th Cir.), cert. denied, 414 U.S. 854 (1973). In other words, once the government establishes that the defendant misappropriated a tangible item that was transported in interstate commerce, the \$5,000 jurisdictional amount may be satisfied by showing that the tangible item contained information worth that much. This applies even where the tangible good transported in

¹¹⁴ At trial the government dismissed the § 2314 count against one of the defendants because it learned that another telephone company was publicly disseminating a computerized text file containing information virtually identical to that the defendant was accused of stealing. Since the information was in the public domain, it could not be a trade secret.

¹¹⁵ There are also at least two other decisions that, in general, support the position that transporting intangible property in interstate commerce violates § 2314. However, both these cases involve the interstate transportation of illegal copies of copyrighted works and their continuing viability is suspect in light of the Supreme Court's decision in United States v. Dowling. In United States v. Belmont, 715 F.2d 459 (9th Cir.), cert. denied, 465 U.S. 1022 (1984), the court held that transporting in interstate commerce illegal "off the air" videotape copies of motion pictures protected by copyright violated § 2314. The court specifically rejected defendant's argument that § 2314 distinguishes between the interstate transportation of "stolen copies" and the interstate transportation of "off the air" copies. See also United States v. Gottesman, 724 F.2d 1517 (2d Cir. 1984). However, as noted, the Dowling Court specifically held that § 2314 does not reach the interstate transportation of unauthorized copies of copyrighted works.

interstate commerce has a de minimis value. For example, this element would be satisfied if a defendant uses a computer diskette worth less than \$1.00 to download a trade secret worth \$5,000.

As discussed more fully above, see "*Trade Secret*," supra p. 74, the value of a trade secret can be established in many different ways. The most direct method, not often available in theft of trade secret cases, is to establish the value of the trade secret on the open market. United States v. Bottone, 365 F.2d 389 (2d Cir.) (value of stolen chemical formulae can be based on what drug manufacturers were willing to pay), cert. denied, 385 U.S. 974 (1966); Greenwald, 479 F.2d at 322. Further, in those matters where the value of the trade secret cannot be established through the use of a "legitimate" market, courts have approved the use of a "thieves" market as a proper means of valuing stolen goods or property under a variety of federal statutes. See e.g., United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988) (18 U.S.C. § 2314); United States v. Drebin, 557 F.2d 1316, 1328 (9th Cir. 1977) (18 U.S.C. § 2314); Churder v. United States, 387 F.2d 825, 833 (8th Cir. 1968) (18 U.S.C. § 641); United States v. Oberhardt, 887 F.2d 790, 793 (7th Cir. 1989) (18 U.S.C. § 641); and United States v. Berkwitz, 619 F.2d 649, 657 (7th Cir. 1980) (18 U.S.C. § 2311). In cases where there is no true market value, i.e., what a willing buyer would pay a willing seller in the open market, federal courts generally find that "any reasonable method may be employed to ascribe an equivalent monetary value," United States v. Drebin, 557 F.2d 1316, 1331 (1972) (quoting United States v. Lester, 282 F.2d 750, 755 (3d Cir. 1960), cert. denied, 364 U.S. 937 (1961)); see also, United States v. Seagraves, 265 F.2d 876, 880 (3rd Cir. 1959). These methods include consideration of the development, research and production costs. See, e.g., United States v. Wilson, 900 F.2d 1350, 1356 (9th Cir. 1990); United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988). But see Abbott v. United States, 239 F.2d 310, 313 (5th Cir. 1956) (value for the purposes of 18 U.S.C. § 2314 is limited to market value.)

(4) Stolen, converted or taken by fraud.

"[T]he terms 'stolen, converted, and taken by fraud' are intended to cover all forms of theft offenses regardless of whether such 'taking' was in the nature of common law larceny." U.S.A.M. 9-61.248; United States v. Lyda, 279 F.2d 461 (5th Cir. 1960); see also United States v. Turley, 352 U.S. 407, 417 (1957) (for purposes of 18 U.S.C. § 2312, "[s]tolen' . . . includes all felonious takings . . . with intent to deprive the owner of the rights and benefits of ownership, regardless of whether or not the theft constitutes common-law larceny.") This broad definition of "stolen" appears to include almost all situations involving the theft of trade secrets. See 2 Milgrim on Trade Secrets § 12.06[2]{c} (1994).

b. *Venue*

Venue for offenses under 18 U.S.C. § 2314 is governed by the provisions of 18 U.S.C. § 3237, and the defendant may be prosecuted in any district where the interstate transportation of the stolen trade secrets was begun, continued, or was completed. See U.S.A.M. 9-61.270.

3. 18 U.S.C. § 2315

Section 2315 addresses receiving stolen property. While § 2314 addresses the transport, transmission or transfer of "goods, wares or merchandise" having a value of \$5,000 or more which have moved in interstate or foreign commerce, § 2315 punishes those who "receive, possess, conceal, store, barter, sell, or dispose" of such property. Because in all other respects § 2314 and § 2315 are substantively identical, the prior discussion on § 2314 should provide guidance on whether a defendant may be prosecuted for knowingly receiving or selling a trade secret under § 2315.

4. 18 U.S.C. §§ 1341 and 1343

The Mail and Wire Fraud statutes can be used to prosecute misappropriation of trade secrets. A detailed discussion of these statutes is beyond the scope of this manual, but it is worthwhile to discuss those elements of §§ 1341 and 1343 that are substantively different in a trade secret case.¹¹⁶

The federal Wire and Mail Fraud statutes proscribe the use of the mails or of interstate or foreign wire transmission, in furtherance of any scheme to defraud, or any scheme for obtaining "property" by false pretenses or representations.¹¹⁷ Appellate courts have upheld convictions

¹¹⁶ For a detailed discussion of 18 U.S.C. §§ 1341 and 1343, readers should refer to Chapter 43 of the U.S. Attorney's Manual and call the Fraud Section of the Criminal Division for further information and guidance.

¹¹⁷ Section 1341 provides in pertinent part as follows:

Whoever, having devised or intending to devise any scheme or artifice to defraud or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises . . . places in any post office or authorized depository for mail any matter or thing whatever to be sent or delivered by the Post Office, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier or takes or receives therefrom any such matter or thing, or knowingly causes to be delivered by mail according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined . . . or imprisoned not more than five

(continued...)

under these statutes for the theft of trade secrets even where no violation of § 2314 was found.¹¹⁸ The broader scope results from the use of the word "property" in the Mail and Wire Fraud statutes as compared to the far narrower phrase "goods, wares and merchandise" used in § 2314. Courts have held that "property" includes intangible property,¹¹⁹ such as trade secrets. See "*Goods, wares or merchandise*," *supra* at p. 87. By contrast, at least one appellate court has held that intangible property does not qualify as goods, wares or merchandise for § 2314. See *United States v. Brown*, 923 F.2d 1301 (10th Cir. 1991), discussed *supra* at p. 88. Thus, these statutes provide a basis for prosecution when mails or wires are used in a misappropriation scheme.¹²⁰

The decision in *United States v. Seidlitz*, 589 F.2d 152 (4th Cir.), *cert. denied*, 441 U.S. 922 (1979), illustrates the use of the Wire Fraud statute in this manner. The defendant used his knowledge of his former employer's computer system to enter the computer system and download computer data. The appellate court upheld the trial court's determination that the stolen data qualified as property within the meaning of the Wire Fraud statute. The court held that the data was a trade secret, even though similar information was in the public domain, because defendant's former employer had "invested substantial sums" to modify the system for its own needs. Further, the information had competitive value, and the employer took steps to prevent persons other than clients and employees from using the system. *Id.* at 160. Accordingly, there was sufficient

(...continued)

years, or both.

Section 1343 provides in pertinent part as follows:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined . . . or imprisoned not more than 5 years, or both.

¹¹⁸ See, e.g., *Abbott v. United States*, 239 F.2d 310 (5th Cir. 1956).

¹¹⁹ See, e.g., *Carpenter v. United States*, 484 U.S. 19 (1987). The defendant in *Carpenter* wrote the "Heard on the Street" column for *The Wall Street Journal*. Although these columns contained no insider information, they had the potential to affect the stock prices of companies discussed in the column because of the "quality and integrity" of the information. The defendant was charged with passing advance information on the columns to two co-conspirators who executed pre-publication trades and earned profits of \$690,000.

The Supreme Court rejected defendant's arguments that he neither interfered with his employer's use of the information, nor disseminated it to the public. The Court held that the defendant had violated the wire fraud statute because the "Wall Street Journal" was the owner of the information contained in the columns and it had been deprived of its right to the exclusive use of the information. 484 U.S. at 26.

¹²⁰ The Mail and Wire Fraud statutes have been identically construed with respect to the issues discussed here. *United States v. Von Barta*, 635 F.2d 999, 1005 n.11 (2d Cir.), *cert. denied*, 450 U.S. 998 (1981) (citing *United States v. Louderman*, 576 F.2d 1383, 1287 n.3 (9th Cir.), *cert. denied*, 439 U.S. 896 (1978)).

evidence from which a jury could conclude that information stored in the computer system was "property" as used in § 1343.

Prosecutors also should consider the applicability of the resurrected "intangible rights theory" found in 18 U.S.C. § 1346 for charging a defendant with fraudulent misappropriation of trade secrets under §§ 1341 or 1343.¹²¹ In such a case, the defendant is charged not with fraudulently obtaining the trade secret, but rather with breaching the fiduciary duty of loyalty he owes to his employer by misappropriating the trade secret. Under this theory, the government must prove that the defendant took steps to actively conceal the misappropriation. The United States is not, however, required to prove that the defendant realized any financial gain from the theft or attempted theft.

Illustrative of this theory is United States v. Kelly, 507 F. Supp. 495 (E.D. Pa. 1981), in which the two defendants were charged with mail fraud for unauthorized use of their company's computer time and storage facilities for the development of a private business venture. The jury found that the defendants defrauded Univac of their loyal and faithful services as employees, and used the mails in furtherance of their scheme. The court denied the defendants' post-trial motions arguing that their convictions should be overturned because the government failed to prove that the goal of the fraudulent scheme was to obtain money or some tangible property right from Univac. The court noted that a private employee may be convicted for mail fraud for failure to render honest and faithful services to his employer if he devises a scheme to deceive, mislead, or conceal material information. The evidence that the defendants violated company policy by extensively using their employer's computer facilities for their own gain, in combination with the steps they took to conceal their use from their employer, was more than sufficient to sustain the conviction.

5. 18 U.S.C. § 1905

Section 1905 statute provides for misdemeanor penalties for government employees who, inter alia, "divulge" or "disclose" government trade secrets. In the only reported decision

¹²¹ In McNally v. United States, 483 U.S. 350 (1987), the Supreme Court held that the mail fraud statute did not include schemes to defraud citizens of their intangible right to honest government, but was limited to protecting "property" rights. In response to this decision, Congress passed 18 U.S.C. § 1346, which provides:

For the purposes of this chapter, the term "scheme or artifice to defraud" includes a scheme or artifice to deprive another of the intangible right of honest services.

This section "may be viewed as restoring the law to its state prior to the McNally decision." United States v. Berg, 710 F. Supp. 438, 442 (E.D.N.Y. 1989); United States v. Johns, 742 F. Supp. 196, 216 (E.D. Pa. 1990) (citing Cong. Rec. H11251 (daily ed. Oct 21, 1988)). See also United States v. Gray, 96 F.3d 769 (5th Cir. 1996). But see United States v. Brumley, 79 F.3d 1430 (5th Cir. 1996) (holding that § 1346 does not restore protection for intangible rights).

involving the disclosure of confidential government information, the court in United States v. Wallington, 889 F.2d 573 (5th Cir. 1989), upheld the defendant's conviction for running background checks on several people who a friend of the defendant suspected of drug dealing.

6. 18 U.S.C. § 1030

Where the defendant acquired information by accessing a "protected computer," prosecutors should consider charging the defendant with a violation of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C) or 1030(a)(4).¹²² Note that neither subsection requires that the information obtained be confidential or secret in nature.

Subsection 1030(a)(2)(C) is designed to protect against the interstate or foreign theft of information by computer. "Information" as used in this subsection is to be broadly construed and includes information stored in intangible form. Moreover, the phrase "obtaining information" includes merely reading it; i.e., there is no requirement that the information be copied or transported. This is important because, in an electronic environment, information can be "stolen" without asportation, and the original usually remains intact.

Section 1030(a)(4) punishes those who misuse computers in schemes to defraud victims of property. This crime proscribes an individual from knowingly and with intent to defraud accessing "a protected computer" without authorization, or exceeding authorized access, and by means of such conduct furthering the intended fraud and obtaining anything of value "unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any one-year period."

The term "protected computer" replaced the term "Federal interest computer" in the most current version of 18 U.S.C. § 1030 and was intended to clarify the breadth of the statute. A protected computer is a computer used exclusively by the United States or a financial institution; one used partly by the United States or a financial institution where the offense affects the government's or financial institution's use of the computer; or any computer which is used in interstate or foreign commerce or communications.

7. State Law

If prosecutors decide not to pursue a case federally, they should consider referring the case to state authorities for prosecution. Many states have laws which specifically address the theft of information, and even if a state does not have such a law, a defendant may often be

¹²² The Computer Fraud and Abuse Act was amended effective October 11, 1996.

successfully prosecuted under a more general theft statute. For a description of state laws in this area see APPENDIX M.

VI. APPENDICES

APPENDIX A: LIST OF CONTACT PERSONS

1. Law Enforcement

Organization	Address	Contact	Comments
Computer Crime and Intellectual Property Section; Criminal Division, U.S. Department of Justice	Suite 200-West Washington Center Building 1001 G Street, NW Washington, D.C. 20001 Tel: (202) 514-1026 Fax: (202) 514-6113	Peter Toren; David Green; Stevan Mitchell	Guidance on intellectual property and computer crimes; coordination of approvals on prosecutions under the Economic Espionage Act.
Federal Bureau of Investigation (FBI); U.S. Department of Justice	J. Edgar Hoover FBI Building Room 3634 935 Pennsylvania Ave., NW Washington, D.C. 20535 Tel: (202) 324-9230 Fax: (202) 324-8072	SSA Julia Conley, Economic Crimes Unit	Oversight of the FBI's Intellectual Property Rights program.
U. S. Customs Service, U.S. Department of the Treasury	Intellectual Property Rights Branch Office of Regulations and Rulings U.S. Customs Service Washington, D.C. 20229 Tel: (202) 482-6960 Fax: (202) 482-6943	John F. Atwood, Chief	Guidance on questions relating to importation of infringing intellectual property.

2. Trademark

Organization	Address	Contact	Comments
International Anti-Counterfeiting Association	1100 Connecticut Avenue NW Suite 1150 Washington, D.C. 20036 Tel: (202) 223-2758 Fax: (202) 872-5848	John Bliss, President	Association representing industries affected by counterfeiting; contact point for obtaining information from corporate victims.
Office of Patents and Trademarks	Commissioner of Patents and Trademarks Box 10 Washington, D.C. 20231 Tel: (800) 786-9199 Fax: (703) 308-7048	N/A	Information on obtaining certified copies of trademark registration.

3. Copyright

Organization	Address	Contact	Comments
Association of American Publishers (AAP)	1718 Connecticut Ave., NW Washington, D.C. 20009-1148 Tel: (202) 232-3335 Fax: (202) 745-0694	Carol Risher	Association representing publishers of reference works; scientific, medical, technical, professional and scholarly books and journals; and classroom instructional and testing materials in print and electronic formats.
Business Software Alliance (BSA)	1150 18th St., NW Suite 700 Washington, D.C. 20036 Tel: (202) 872-5500 Fax: (202) 872-5501	Bob Kruger	Association representing large vendors who make computer software for business and personal use.
Interactive Digital Software Alliance (IDSA)	1130 Connecticut Ave., NW Suite 710 Washington, DC 20036 Tel: (202) 833-4372 Fax: (202) 833-4431	Kathlene Karg	Association representing vendors of interactive entertainment software for all platforms, including personal computers, video game cartridges and video game compact disks.
Motion Picture Association of America (MPAA)	15503 Ventura Boulevard Encino, CA 91436 Tel: (818) 995-6600 Fax: (818) 382-1785	Ed Pistey	Association representing the film and entertainment industry.

Organization	Address	Contact	Comments
Recording Industry Association of America (RIAA)	1020 19th St., NW Suite 200 Washington, D.C. 20036 Tel: (202) 775-0101 Fax: (202) 775-7523 Fax: (202) 775-7253	Frank Creighton	Association representing manufacturers of sound recordings in all formats.
Software Publisher's Association (SPA)	1730 M Street NW Suite 700 Washington, D.C. 20036 Tel: (202) 452-1600 Fax: (202) 223-8756	Rodolfo Orjales	Association representing computer software vendors.
Library of Congress	Library of Congress Copyright Office Certifications and Documents LM 402 Washington, D.C. 20559 Tel: 202-707-3000	N/A	Information on requests for certified copies of copyright registration.

APPENDIX B: SAMPLE INDICTMENT - 18 U.S.C. § 2319

**WILLFUL INFRINGEMENT OF COPYRIGHT (MISDEMEANOR)
(17 U.S.C. § 506(a) and 18 U.S.C. § 2319(b)(3))**

On or about the _____ day of _____, 19____, in the _____ District of _____, the defendant _____, did willfully and for purposes of commercial advantage and private financial gain infringe the copyright's of various copyrighted works, to wit, [describe works infringed], in that the defendant _____, did [describe manner of infringement] (e.g., reproduce, distribute)], without authorization of the copyright holder.

All in violation of Title 17, United States Code, Section 506(a) and Title 18, United States Code, Section 2319(b)(3).

APPENDIX C: SAMPLE INDICTMENT - 18 U.S.C. § 2319

**WILLFUL INFRINGEMENT OF COPYRIGHT (FELONY) --
REPRODUCTION OR DISTRIBUTION
(17 U.S.C. § 506(a) and 18 U.S.C. § 2319(b)(1))**

From on or about the ____ day of _____, 19____, and continuing until on or about the ____ day of _____, 19____, in the _____ District of _____, the defendant _____, did willfully and for purposes of commercial advantage and private financial gain, infringe the copyrights of various copyrighted works, to wit, [describe works infringed], in that the defendant _____ did (reproduce or distribute) [insert number or "at least 10"] copies (or phonorecords), within a 180-day period, with a retail value of more than \$2,500, without authorization of the copyright holder.

All in violation of Title 17, United States Code, Section 506(a) and Title 18, United States Code, Section 2319(b)(1).

APPENDIX D: SAMPLE INDICTMENT - 18 U.S.C. § 2320

**TRAFFICKING IN COUNTERFEIT GOODS OR SERVICES
(18 U.S.C. § 2320)**

On or about the ____ day of ____, 19 __, in the ____ District of ____, the defendant ____,
did intentionally traffic and attempt to traffic in goods, to wit [describe counterfeit goods], in
connection with which counterfeit marks were used that were identical with and substantially
indistinguishable from genuine marks in use and registered for those goods on the principal
register in the United States Patent and Trademark Office, and the use of which counterfeit marks
was likely to cause confusion, to cause mistake, and to deceive.

All in violation of Title 18, United States Code, Section 2320.

APPENDIX E: SAMPLE INDICTMENT - 18 U.S.C. § 1831

**ECONOMIC ESPIONAGE
(18 U.S.C. § 1831)**

On or about the ____ day of _____, 19____, in the _____ District of _____, the defendant _____, did knowingly steal and without authorization [describe the misappropriation] a trade secret, to wit, [describe trade secret], owned by [name of owner], intending and knowing that the [describe the misappropriation] would benefit a foreign government, foreign instrumentality and foreign agent.

All in violation of Title 18, United States Code, Section 1831.

APPENDIX F: SAMPLE INDICTMENT - 18 U.S.C. § 1832

**THEFT OF TRADE SECRETS
(18 U.S.C. § 1832)**

On or about the ____ day of _____, 19 ____, in the _____ District of _____, the defendant _____, did steal and without authorization [describe the misappropriation] a trade secret, to wit, [describe trade secret], that is related to and included in a product that is produced for and placed in interstate and foreign commerce, owned by [name of owner], knowing that the [describe the misappropriation] would economically benefit someone other than the owner thereof, and intending and knowing that the [describe the misappropriation] would injure [name of owner].

All in violation of Title 18, United States Code, Section 1832.

APPENDIX G: SEARCH WARRANT AFFIDAVIT (Electronic Environment)

AFFIDAVIT OF SPECIAL AGENT

1. INTRODUCTION

"Agent," a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, deposes and states:

1. I have been a Special Agent of the FBI for approximately four years. I am assigned to the investigation of white-collar crimes in the Anywhere, U.S.A. area, and in particular to the investigation of crimes involving computer fraud and abuse. For approximately the last three years, I have been a field examiner for the FBI forensic laboratory's Computer Analysis and Response Team, which specializes in searching for and analyzing evidence stored on computers. I make this affidavit in support of an application by the United States of America for the issuance of a warrant to search the apartment at "TARGET" for evidence of, and property designed or intended for use, or which is or has been used as the means of committing (hereafter referred to as "instrumentalities"), violations of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 2319 and 2 (criminal copyright infringement), as well as the fruits of this crime, and property criminally possessed -- namely copyrighted computer software.

2. During my career as a Special Agent of the FBI, I have participated in numerous investigations involving computer-related offenses, and have participated in the execution of approximately 20-25 search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have personally submitted affidavits in connection with approximately five searches in computer-crime cases. I have interviewed numerous persons involved in the unlawful use of computers to traffic in stolen software, access devices (including credit card numbers and computer passwords), and other electronically-stored property, and have analyzed computer hardware and software recovered during the execution of search warrants. Additionally, I have received both formal and informal training in the field of computers and telecommunications from the FBI and various telecommunications service providers.

3. This affidavit seeks the issuance of a search warrant for the residence of TARGET who is the subject of an investigation currently being conducted by the FBI. As set forth in more detail below, there is probable cause to believe that the subject has committed and is continuing to commit criminal copyright infringement, and that he maintains at his residence computers, electronic equipment, software programs, storage media, records, and other evidence and instrumentalities of his criminal activities as described more fully herein.

II. CRIMINAL VIOLATIONS

4. This affidavit seeks a search warrant to obtain evidence of criminal copyright infringement. Title 17, United States Code, Section 506(a) provides that "any person who infringes a copyright willfully and for purposes of commercial advantage or private financial gain shall be punished as provided in section 2319 of Title 18." Title 18, United States Code, Section 2319(b)(1) provides that any person who violates 17 U.S.C. § 506(a):

shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, with a retail value of more than \$2,500.

III. SOURCES OF INFORMATION RELATED IN THIS AFFIDAVIT

5. I make this affidavit in part from personal knowledge based on my participation in this investigation, including witness interviews and my review of documents and tape-recorded conversations, in part on information gained through my training and experience, and in part on information received from "LAWYER" told me that he is an attorney who represents XYZ Corporation, of Anywhere, U.S.A. in matters relating to the alleged infringement of the copyright on XYZ Corporation's "XYZ Software." Both _____ and _____ told me that _____ of Anywhere, U.S.A., is a technical expert retained by to assist in evaluating alleged infringement of XYZ Corporation's copyright in the XYZ Software. According to a resume, provided to me by _____, _____ is experienced in software development and in the forensic examination of computer software and hardware in connection with copyright infringement disputes.

6. Because this affidavit is being submitted for the limited purpose of seeking authorization for a warrant to search the premises at _____ I have not set forth each and every fact learned during the course of this investigation. Facts not set forth herein are not being relied upon in reaching my conclusion that a search warrant should be issued.

IV. THE PREMISES FOR WHICH A SEARCH WARRANT IS SOUGHT

7. This affidavit is submitted in support of an application to search the residence at _____. This residence is located within a multi-unit light brick apartment building on the east side of _____ Street. The exterior of the residence is depicted in the photograph attached as Exhibit A to this affidavit.

8. Telephone records reflect that telephone numbers _____ and _____ are located at _____ and subscribed by _____.

9. Records of the Secretary of State, Driver's License Division, reflect that _____ resides at _____ and was born on _____.

**THERE IS PROBABLE CAUSE TO BELIEVE THAT TARGET
HAS COMMITTED AND IS CURRENTLY COMMITTING
CRIMINAL COPYRIGHT INFRINGEMENT, AND THAT
EVIDENCE AND INSTRUMENTALITIES OF THIS OFFENSE
WILL BE FOUND AT THE SUBJECT PREMISES**

Description of the Criminal Activities

10. As set forth in more detail below, TARGET operates a computer BBS known as PIRATE BBS that illegally traffics in copyrighted computer software. Persons gain access to this BBS by providing (or "uploading") files, including copyrighted software files, obtained from other sources, and in turn are permitted to copy (or "download") files provided by other users. I have reviewed a directory of the files available on the PIRATE BBS as of _____. That directory includes numerous commercially marketed software products, which I believe from my experience and training to be protected by copyright. As reflected in the directory of files available on the PIRATE BBS, the number of copyrighted software products copied onto that BBS and available for further copying by BBS users is substantially in excess of ten; additionally, based on my acquaintance with the retail prices of software products, the combined retail value of the copyrighted products available through the PIRATE BBS is substantially in excess of \$2,500.

11. One of the products which the PIRATE BBS directory lists as available for downloading by BBS users is "XYZ Software," communications software developed, published, and copyrighted by XYZ Corporation, and which sells at retail for approximately \$_____ per copy. A page of XYZ Software, which is displayed to the user when the software is first loaded, prominently displays notice of XYZ Corporation's copyright. The posting of XYZ Software and other copyrighted software on the BBS infringes software copyrights and enables and users of his PIRATE BBS to obtain large volumes of expensive software without payment.

12. XYZ Corporation, based in Anywhere, U.S.A., is in the business of designing, developing, manufacturing, marketing, and supporting software that enables IBM personal computers and compatible models to communicate with one another, through modems, on telephone lines. XYZ Corporation's products, marketed under the "XYZ Software" name, are well-known in the computer industry.

13. On _____ [date] XYZ Corporation released a product titled "XYZ Software" This product was an enhanced version of an earlier XYZ Software product intended for use in conjunction with the Windows operating software produced by the Microsoft Corporation. According to XYZ Corporation's attorney, _____, the preceding release of XYZ Software generated revenues for XYZ Corporation totaling approximately \$15,000,000 during the year following its first release in May 1993. LAWYER stated that during 1993 and the first half of 1994, XYZ Corporation spent approximately \$2,000,000 to develop XYZ Software.

14. I have reviewed a Certificate of Registration issued by the U.S. Copyright Office

for XYZ Software. That certificate, effective [date], reflects the date of first publication of the work as [date]. Title 17, United States Code, Section 412 permits registration of a work within three months of its first publication. According to _____, XYZ Corporation is the sole owner of all interests in the copyright for XYZ Software.

15. As is the case with software published by many software companies, persons who purchase copies of XYZ Corporation products, including XYZ Software, do not purchase the software itself, but merely a license to use a copy of the software. The license that accompanies packages of XYZ Corporation software authorizes purchasers to use the software on a single machine at a single site, at any one time.

16. On August 23, 1994, I participated in the execution of a search warrant at the residence of COOPERATING WITNESS ("CW") in _____, [state]. In the course of my investigation of the activities of _____, including the seizure of the computer and storage media used to operate the ABC BBS, I determined that the ABC BBS provided a forum for the illegal copying and distribution of large numbers of copyrighted software files, and served approximately [number] users. After the execution of the search warrant, CW agreed to assist in the FBI's investigation into the use of computer BBSs to illegally copy and distribute copyrighted software in the area, and to provide information about other BBSs that illegally traffic in large numbers of copyrighted files. Such BBSs are commonly known as "pirate BBSs".

17. CW informed me that one pirate BBS with which he is familiar is the PIRATE BBS. CW told me that he learned of the PIRATE BBS from the person who helped him start the PIRATE BBS, and that this person provided CW with the telephone number for the PIRATE BBS and agreed to serve as a reference for CW as CW sought access to the PIRATE BBS. I know from my experience that many BBSs which illegally traffic in copyrighted software require that someone seeking to become a new user first provide references from persons known to the system operator ("sysop") of the BBS.

18. CW told me that the PIRATE BBS required new users to upload what referred to as "elite" files to gain access to the BBS. According to CW and to others with whom I have spoken who are knowledgeable about "pirate" BBSs, the term "elite" is commonly used to refer to commercially-sold, copyrighted software. CW told me that in operating his own BBS, he likewise required prospective new users to upload "elite" files before gaining access to the BBS. CW told me that he uploaded files to the PIRATE BBS on multiple occasions, and in return was allowed to download files from the PIRATE BBS. CW told me that he had never met or spoken by voice with the sysop of the PIRATE BBS, but that the sysop used the pseudonym "_____."

19. On [date] I was present as CW used a computer equipped with a modem to dial telephone number _____. After gaining access to the PIRATE BBS at that telephone number, CW printed the computer screens that appeared before him during this login session. I have attached as Exhibit B to this Affidavit the series of screen prints that CW made during this login session. Because of the way that CW printed out the screens, more than one screen of

information ordinarily appears on a single printed page, and screens often spill from one printed page to the next. Additionally, graphic images and charts often appear in distorted form, and some text lines are truncated.

20. The screen displayed after _____ user name and password was accepted welcomed user " _____ " -- _____ user name -- and identified him as user number _____. I know from my training and experience that BBSs commonly identify users by a number, in addition to a name. The fact that _____ is user _____ suggests that the PIRATE BBS has had at least _____ other users. This welcoming screen provided certain basic account information for _____, and noted that he had called the BBS _____ times, and that his account permitted him " _____ calls, using a maximum of _____ minutes per day."

21. Another screen, which carried the legend " _____ BBS, (c) 1992 _____," noted that "extra credit" would be given for the seventeen files listed below. The files on the list were identified as "Elite File Bases." I understood this to mean that persons who uploaded these files would receive in return more than the usual credits to use for downloading other files. The files on this list included the following commercially-available software, which I believe from my experience and training are likely to be protected by copyright:

P.C. Anywhere version 5.0
Adobe Photoshop version 3.0
dBase for Windows.

The list also solicits what is identified as "Ill. Licince plate databas" [sic]. Because this list was displayed on the screen in chart form, it appears in a distorted format in Exhibit B.

22. Later in the day I was present as _____ used a computer equipped with a modem to dial telephone number _____. _____ login session was captured through a utility function and stored on a screen-by-screen basis. A printed record of that login session is attached as Exhibit C to this Affidavit. As before, a welcoming screen welcomed users to the PIRATE BBS and identified the sysop as "_____". A "general message" to all users from _____, identified as user number one, solicited applicants for a position as "file co-sysop." According to the message, this position would involve assisting in deleting old and duplicate files, sorting through uncategorized files, and providing other assistance in the operation of the PIRATE BBS. The message stated that in return, the co-sysop "will be given access to node #3 and unlimited downloads, for as long as you continue to do the job." The message asked interested parties to reply to _____ by the electronic mail feature on the BBS. This message indicates to me that the person using the pseudonym " _____ " has primary control of the PIRATE BBS.

23. The bulk of Exhibit C consists of listings of files available for downloading from the PIRATE BBS. As Exhibit C reflects, the files available for downloading from the PIRATE BBS are grouped by subject matter and organized into directories. A listing of 79 directories on

the PIRATE BBS appears in Exhibit C. Many of these directories contain the word "elite" -- for example, one directory is titled "Elite Utilities [A-M]," another "Elite Windows," and another "Elite OS/2 & NT." (Windows and OS/2 are commonly-used computer operating systems.) Numerous other directories begin with the words "Elite Games," followed by a subcategory of game programs stored in each directory. The directory also lists 27 different entries for "Elite Tape," reflecting files stored offline on tape, and available for downloading upon request. On the basis of my training and experience, and my review of the contents of the directories as listed in Attachment C to this Affidavit, I believe these directories of "elite" files consist substantially or wholly of copyrighted software files.

24. I have reviewed the index of software available on the PIRATE BBS as captured in _____ second login session on [date]. That index (included as part of Exhibit C to this affidavit) contains an extensive listing of commercially available software products, many of which retail for hundreds of dollars. The following is a partial listing of the well-known commercially marketed software reflected on the index as available for downloading through the PIRATE BBS, and which I believe from my experience and training are likely to be protected by copyright:

- Cadkey 6.0
- DOS version 6.22 Step-Up
- Borland's dBase version 5.0
- Dbase 5.0
- Harvard Graphics 3.0 for DOS
- Harvard Graphics for Windows version 2.0
- Autodesk Home
- Instant Artist by Autodesk
- Labelmaker Pro
- Listen 2.0 from Verbex
- Lotus Magellan version 1.0
- Modem Doctor version 5.2
- Norton Desktop for DOS
- Procomm Plus for Windows version 2.1
- Procomm Plus for Windows version 2.0
- Procomm Plus version 2.01
- Print Artist version 2.0 by Maxis
- Adobe Photoshop 3.0
- Doom II
- Tony LaRussa Baseball 2
- Mickey's Follow the Reader by Disney
- Powerbuilder version 3.0
- Microsoft Access version 2.0
- AutoMap Pro version 1.06 for Windows
- Corel Draw version 4.0
- Corel Draw version 5.0

Matematica 2.1 for Windows
Matematica 2.2 for Windows
Lion King Graphics for Print Shop for Windows
Powerpoint version 4.0
Microsoft Windows 4.0 (Chicago release- Beta version)
WordPerfect 6.0a for Windows
WordPerfect 6.0
WordPerfect 5.1+
MS-Works version 3.0
OS/2 for Windows, upgrade to 2.11
Ami Pro for OS/2 version 3.0a
American Heritage Dictionary
Norton's PC Anywhere version 4.5
Intel's Application Builder for Windows
Word for Windows 2.0
Norton Utilities 7.0
Microsoft Visual Basic version 2.0 Professional Edition
Microsoft Windows version 3.1
Morph Image Processor for Windows
Where in Space is Carmen San Diego?
Adobe Illustrator version 4.0
Freelance Graphics version 2.0
PC Tools for Windows
XTree Gold for DOS version 2.51
Auto Cad version 12
Betty Crocker Cookbook
Paradox version 4.2
Powerpoint 3.0
Windows for Work Groups version 3.1
Microsoft Visual C++ Pro Edition
Windows NT
Quicken version 7.0 for DOS
Quicken for Windows version 3.0
Borland Turbo C++
Lotus Notes version 3.0
Lotus Notes version 3.0 for OS/2
Microsoft DOS version 6.2
Webster's Online dictionary
Norton Desktop for Windows version 3.0
Procomm for OS/2 version 2.1
SQL Windows 4.0 Development System - Corporate
Microsoft Excel Version 5.0
Avery Label Pro for Windows

25. During his second login session on [date], CWdownloaded the files identified on the PIRATE BBS directory as containing XYZ Software. I provided those files to _____, who subsequently told me that _____ had analyzed them and determined that those files contain an exact copy of the XYZ Software software whose copyright is owned by XYZ Corporation. _____ told me that the copy of XYZ Software 2.0 posted on the PIRATE BBS is an unauthorized and therefore infringing copy, and that neither _____ nor the PIRATE BBS have been authorized by XYZ Corporation to distribute any XYZ Corporation software.

26. On [date], I used a modem to dial _____, and connected to a the PIRATE BBS. Rather than logging on using _____ name and password, I attempted to gain access to the system as a member of the public, and followed the instructions for logging on as a "guest." After completing this procedure I received the following message:

You are currently logged in as GUEST. While you will be able to browse the system, there are several limitations on what you can do:

- 1) You cannot access the online games.
- 2) Although you can leave private mail, you cannot receive a response.
- 3) You may not post private messages.

If you are interested in an account, please log off and log back on using your handle.

27. Shortly afterwards a screen informed me that as "guest" my use was limited to two calls, using a maximum of 20 minutes per day. I invoked certain of the options available from the main menu, and determined that I was able to read messages posted in a "General Messages" area, and that I was able to view a list of files in an area captioned "Archive Programs." Before I attempted to download any files, or to gain further access to lists of files available through the BBS, my connection to the PIRATE BBS was involuntarily terminated. I called the PIRATE BBS again and logged in as "guest," but after a brief period my connection with the BBS was involuntarily terminated. I did not attempt further access in order to avoid arousing the suspicions of the sysop.

28. On [date], I again used a modem to dial _____, and connected to the PIRATE BBS. Rather than logging on using _____ name and password, or as a "guest," I followed the instructions for logging on as a new user. After completing this procedure I received the following message:

New users start with very limited access to this system. However, just leave a message requesting validation of the _____ (#1) and in most cases you'll be given normal user access in 24-48 hours.

New user restrictions:

1. You are only allowed only 15 minutes on-line.
2. Your public mail must be validated before it is available.
3. You cannot vote.

29. Shortly after viewing the above screen, I received a message which read in part as follows:

You are not currently a validated user. The most likely causes are either that you have neglected to write a note to ____ (#1) requesting validation, or he has not gotten to it yet.

Another message informed me that as a user who had not been validated, my access was limited to two calls, using a maximum of twenty minutes per day.

30. I continued on the PIRATE BBS, and was allowed access to the main menu. I selected the menu option labeled "File system," and invoked a subsequent menu option to display a file "area list." The BBS then displayed a list of approximately 139 file sections, many of whose titles suggested that they contained software files. Among the file areas appearing on this list were the following: <Novell> Communications; <Novell> Netware; <CD> Windows Files; <CD> Word Processors & Utilities; <CD> Utilities [A-F]; <CD> Utilities [G-L]; <CD> Utilities [M-Q]; <CD> Utilities [R-Z]; <CD> Procomm Communications Files; <CD> Lotus 123 v1&2&3 Files; and <CD> Wordperfect Files & Help. The initials "CD" before a file area may indicate that files in that area are stored on a compact disk accessible through the BBS.

31. I selected the menu option for "Word Processors & Utilities," and received the following message: "Sorry, that section is only available to validated users." I did not attempt further access to file areas in order to avoid activity that might arouse the suspicion of the sysop.

32. During my session on the PIRATE BBS on [date], at several points I viewed a screen identifying the BBS as the ____ BBS and bearing the notice "© 1992 ____."

33. On the basis of this login session and the information recited earlier in this affidavit, I believe the PIRATE BBS operates essentially as a private club, which restricts membership and full access to those individuals personally approved by ____, and who demonstrate their trustworthiness by uploading proprietary software. Because of the restrictions on full access, which include limits on the use of electronic mail, the ____ BBS tends to serve as a mode of private communication for a small and secretive group of members, rather than as a mode of public communication such as a book, newspaper, or public broadcast.

34. Based on my review of the records of CW's sessions on the PIRATE BBS, my own sessions on the PIRATR BBS, my interviews with ____ and ____, the information recited

in this warrant application, and my experience and training, I believe that the PIRATE BBS constitutes property which is designed and/or intended for use and which is being and has been used as the means of committing numerous criminal copyright violations by the operators and users of the _____ BBS.

**Basis to Search Previously Opened and Stored Communications
Relating to Sysop Messages, E-Mail, and Conference Functions**

35. The menus for the PIRATE BBS reflect that in addition to containing files for downloading, the BBS enables users to (among other activities) send private messages and "chat w/ sysop."

36. Most BBS software with which I am familiar allows users to save private communications once those communications have been opened. Because the principal purpose of the PIRATE BBS appears to be to traffic in software, including copyrighted software, I believe much of the electronic correspondence among users is likely to relate to the uploading and downloading of software.

37. With respect to communications between the sysop and individual users, I believe such correspondence is likely to include messages from the sysop to users about the operation of the PIRATE BBS, inquiries by users about the sysop's interest in particular software, requests from users to download software that is stored offline, requests from new users for access to the PIRATE BBS, information about other BBS's which also trade copyrighted software, and comments and questions about the operations of the PIRATE BBS and software available on the PIRATE BBS. Such communications will tend to establish the identity of the sysop and the extent of the sysop's knowledge of the contents and operation of the PIRATE BBS, including the posting of contraband copyrighted software. As noted in paragraph 22 above, one example of the use of such communications in furtherance of the illegal trafficking of copyrighted software is the general message that I saw on [date], which solicited applicants for a position as "file co-sysop" and promised "unlimited downloads, for as long as you continue to do the job," and asked interested parties to respond to the sysop by e-mail.

38. With respect to communications between users who are not sysops, I believe such communications are likely to include comments and questions about the operation of the PIRATE BBS and about software available on the PIRATE BBS, and information about other BBS's which also trade copyrighted software. Such communications between users ordinarily are accessible by the sysop.

39. For the reasons set forth above, I believe there is probable cause to search for and seize any and all previously opened and stored communications between users (including sysops), as well as all unopened communications to or from sysops. This application does not seek authority to open or read unopened private communications between users who are not sysops.

40. I know from my training and experience that the "chat w/ sysop" feature reflected on the main menu of a BBS such as the PIRATE BBS ordinarily allows users to communicate with the sysop in real time, in the manner of a conversation. The communications displayed in such a chat sometimes are stored on the BBS. Because the principal purpose of the PIRATE BBS appears to be to illegally traffic in copyrighted software, I believe it is likely that any such stored conversations would pertain or be relevant to that activity. Accordingly, I believe there is probable cause to search for and seize any and all stored records of on-line electronic communications between sysops and users of the PIRATE BBS.

41. The records of [date] login sessions on the PIRATE BBS reflect that in addition to the numerous sections of the BBS containing copyrighted software files available for downloading, the PIRATE BBS also has file sections with titles suggesting that the PIRATE BBS also may be used for communications which do not involve the illegal trafficking of copyrighted material. Some of these file areas, as identified in a listing contained in Exhibit B, are as follows: "PC Magazine Utilities;" "Other Magazines and Newsletters;" "Food & Recipes;" "Humorous Text & Programs;" and "The Bible & Other Lies." The names of these file sections appear near the end of the listing of file sections, and after the listings of numerous file sections containing software files. Whether these file directories contain copyrighted material is unknown. Because of the vast quantity of material available through the PIRATE BBS, it will not be practical to conduct an on-site review of all sections of the PIRATE BBS during the execution of the search warrant to determine whether some sections of the BBS do not involve the illegal trafficking of copyrighted material.

Basis to Search the Subject Premises and Items to be Seized

42. I believe that there is probable cause to believe that evidence of the above-described criminal activities will be found at the residence of _____. This conclusion is based on my experience and training relating to the types of records and items that persons engaged in the activities described above typically keep at their residences, as well as on the facts recited above.

43. Persons who operate BBS's at their residences or elsewhere often maintain at the location from which the BBS is operated items tending to show ownership or control of the premises from which a BBS is operated, such as bills, letters, invoices, personal effects, and legal documents.

44. The operation and maintenance of a BBS trafficking in contraband property such as copyrighted software involves the use of computer-related property that includes computer hardware, computer software, computer-related documentation, passwords, and data security devices. (Each of these categories is further defined below.) Such property is used to physically establish, operate, and secure the BBS, and to provide the stock-in-trade for the trafficking that takes place on the BBS.

45. Computer hardware, computer software, computer-related documentation, passwords, and data security devices may be used by one engaging in criminal copyright infringement in two distinct respects: (1) as instrumentalities for the violation of federal copyright infringement laws through the reproduction and distribution of copyrighted material; and (2) as devices used in conjunction with the collection and storage of electronic data and records which constitute evidence of that offense. Search and seizure of computer hardware, software, documentation, passwords, and data security devices, either as instrumentalities of criminal activity or as evidence thereof, is contemplated in and permitted by Rule 41 of the Federal Rules of Criminal Procedure.

Items to be seized as instrumentalities

46. Computer hardware is described as any and all computer equipment, including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

47. Computer software is described as any and all information, including any instructions, programs, or program code, stored in the form of electronic, magnetic, optical, or other media which are capable of being interpreted by a computer or its related components. Computer software may also include certain data, data fragments or control characters integral to the operation of computer software. These items include but are not limited to operating system software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

48. Computer-related documentation is described as any written, recorded, printed or electronically stored material which explains or illustrates the configuration or use of any seized hardware, software, or related item.

49. Computer passwords and data security devices are described as all those devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to or facilitate concealment of any computer hardware, computer software, computer-related documentation, electronic data, records,

documents or materials within the scope of this application. These items include but are not limited to any data security hardware (such as any encryption devices, chips and circuit boards), passwords, data security software or information (such as test keys and encryption codes), and similar information that is required to access computer programs or data or to otherwise render programs or data into a useable form.

50. As set forth above, computers have been and are being used to operate the PIRATE BBS, and to store and distribute infringing copies of copyrighted software. Therefore, the above-mentioned computer hardware, software, computer documentation, passwords and data security devices constitute means of committing criminal offenses, and are thus instrumentalities in (as well as evidence of) the violations recited herein. These materials are therefore subject to seizure pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and may be retained as evidence and as instrumentalities used in the commission of a crime for a reasonable period of time and may be examined, analyzed, and tested as evidence and instrumentalities used in the commission of a crime for a reasonable period of time.

Items to be seized as evidence

51. In addition to his use of computers as instrumentalities of the offense of criminal copyright infringement, _____ has used and is using computers and related electronic storage devices to collect, store, maintain, retrieve, conceal, transmit, and use electronic data in the form of electronic records, documents, and materials, including those used to facilitate communications -- which together and separately constitute evidence of the offense of criminal copyright infringement. This data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment. This media includes but is not limited to any fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

52. The phrase "records, documents, and materials, including those used to facilitate communications" as used in paragraph 43 above includes but is not limited to records of personal and business activities relating to the operation of a BBS engaged in the trafficking of software, such as: associate names and addresses (as contained in, among other things, telephone and address records of BBS users, associates, suppliers, and customers); the identity and location of assets illegally gained through criminal activity (including but not limited to any invoices, receipts, bank account records, income tax returns, telephone records and correspondence); information regarding sources of software; software lists; technical information relating to software trafficked on the BBS; correspondence; and information about the operations of other BBSs engaged in similar activities. Such information is typically contained in notes, logbooks, diaries, address books, ledgers, telephone records, bank records, income tax returns, receipts, invoices, and reference materials.

53. The phrase "records, documents, and materials, including those used to facilitate

software, to insure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, Bernoulli drives, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data analysis "on-site."

b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

58. Due to the volume of the data at issue and the technical requirements set forth above, it is usually necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. It may be the case, however, under appropriate circumstances, that some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such -- or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readily, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. The records of CW and my sessions on the PIRATE BBS reflect that the volume of information stored on the computer hardware used to operate that BBS is likely to be too extensive to analyze appropriately without removing that hardware from _____ residence.

VI. CONCLUSION

WHEREFORE, I respectfully request that the search warrant be issued as applied for herein.

Special Agent, FBI

Subscribed and sworn to
before me this ____ day
of _____:

United States Magistrate Judge

**APPENDIX H: SAMPLE LANGUAGE FOR JURY INSTRUCTIONS -
18 U.S.C. § 2319**

**CRIMINAL COPYRIGHT INFRINGEMENT
OFFENSE INSTRUCTION
(17 U.S.C. § 506(a))**

The indictment charges a criminal violation of the Copyright Act. The Copyright Act provides that "[a]ny person who infringes a copyright willfully and for purposes of commercial advantage or private financial gain" shall be guilty of an offense against the United States.

Source: 17 U.S.C. § 506(a)

United States v. Cross, 816 F.2d 297, 303 n. 2 (7th Cir. 1981)

ELEMENTS OF THE OFFENSE--
WILLFUL INFRINGEMENT OF COPYRIGHT (FELONY)¹²⁴
(17 U.S.C. § 506(a) and 18 U.S.C. § 2319(b)(1))

The defendant is charged in [Count _____ of] the indictment with criminal copyright infringement in violation of Section 506 of Title 17 and Section 2319(b)(1) of Title 18 of the United States Code. In order for the defendant to be found guilty of this charge, the government must prove each of the following elements beyond a reasonable doubt:

First, that there exists a valid copyright for [describe work(s) in question];

Second, that at the time and place alleged, the defendant infringed the copyright(s) in [the work(s)] by [reproducing] [distributing] copies of [the work];

Third, that the defendant, in infringing the copyright(s), acted willfully;

Fourth, that the acts of infringement were for the purpose of commercial advantage or private financial gain;

Fifth, that at the time and place alleged, the defendant, in infringing the copyright(s), [reproduced] [distributed] at least 10 [copies] [phonorecords] of [the work];

Sixth, that the copies or phonorecords [reproduced] [distributed] had a retail value of more than \$2,500.

¹²⁴ These model instructions do not discuss the first sale doctrine. As noted, there is disagreement among the courts regarding the proper role of the first sale doctrine in criminal copyright cases. See “*The first sale doctrine in criminal cases*,” *supra* at 27. Accordingly, we have not included instructions which specifically relate to the first sale principle. Prosecutors seeking assistance in tailoring appropriate first sale instructions are encouraged to contact the Computer Crime and Intellectual Property Section for assistance.

ELEMENTS OF THE OFFENSE INFRINGEMENT

The second element of the offense charged is infringement. An infringement of a copyright occurs whenever someone who is not the copyright owner and who has no authorization from the owner does an act which is the exclusive right of the copyright owner to do. Among the exclusive rights given to the owner of a valid copyright are the rights to [reproduce, distribute] the copyrighted work. In this case, the Government alleges that the defendant infringed the copyright by [reproducing, distributing] [the work in question].

If you find that the defendant [reproduced, distributed] [the work in question] without the authorization of the copyright owner, then you may find that the defendant infringed the copyright in [the work in question].

Source: 17 U.S.C. §§ 106, 501

United States v. Cross, 816 F.2d 297, 303 n. 2 (7th Cir. 1987)

United States v. Wise, 550 F.2d 1180, 1186 (9th Cir.),
cert. denied, 434 U.S. 929 (1977)

ELEMENTS OF THE OFFENSE
COMMERCIAL ADVANTAGE OR PRIVATE FINANCIAL GAIN

The fourth element of a copyright infringement is that the alleged infringement was done for the purpose of commercial advantage or private financial gain. With respect to this element, you are instructed that the Government need not prove that the defendant actually received a profit from the infringement. The Government need only show that the defendant acted with the hope or expectation of some commercial advantage or financial gain.

If you find that the defendant infringed the copyright in [the work in question] with the hope or expectation of some financial gain, then you may find that the defendant's infringement was done for the purpose of commercial advantage or private financial gain.

Source: United States v. Moore, 604 F.2d 1228 (9th Cir. 1979)
United States v. Wise, 550 F.2d 1180 (9th Cir.),
 cert. denied, 434 U.S. 929 (1979)

**APPENDIX I: SAMPLE LANGUAGE FOR JURY INSTRUCTIONS -
18 U.S.C. § 2320**

**TRAFFICKING IN COUNTERFEIT GOODS OR SERVICES
(18 U.S.C. § 2320)**

The defendant is charged in [Count _____ of] the indictment with trafficking in counterfeit goods or services in violation of Section 2320 of Title 18 of the United States Code. In order for the defendant to be found guilty of this charge, the government must prove each of the following elements beyond a reasonable doubt:

First, that the defendant trafficked or attempted to traffic in goods or services;

Second, that such trafficking, or attempt to traffic was intentional;

Third, that the defendant used a "counterfeit mark" on or in connections with such goods or services; and

Fourth, that the defendant knew that mark so used was counterfeit.

ELEMENTS OF THE OFFENSE
TRAFFICKING IN GOODS OR SERVICES

The first of these elements is that the defendant trafficked or attempted to traffic in goods or services.

The term "traffic" means to transport, transfer, or otherwise dispose of, to another, as consideration for anything of value, or make or obtain control of with intent so to transport, transfer or dispose of. In this case, the Government alleges that the defendant trafficked by [describe] [the goods or services in question].

If you find that the defendant [describe] [the goods or services in question], then you may find that the defendant trafficked in goods or services.

Source: 18 U.S.C. § 2320

ELEMENTS OF THE OFFENSE
TRAFFICKING WAS INTENTIONAL

The second element of the offense charged is that the defendant's trafficking was intentional. The trafficking was intentional if the defendant acted deliberately or on purpose. With respect to this element, you are instructed that the Government need not prove that the defendant intended to violate the law. The Government need only show that the defendant acted on purpose.

If you find that the defendant's trafficking was deliberate or done on purpose, then you may find that the defendant's trafficking was intentional.

Source: 18 U.S.C. § 2320

United States v. Baker, 807 F.2d 427, 429 (5th Cir. 1986)

United States v. Gantos, 817 F.2d 41, 42-43 (8th Cir.),
cert denied, 484 U.S. 860 (1987)

ELEMENTS OF THE OFFENSE COUNTERFEIT MARK

The third element is that defendant used a counterfeit mark on or in connection with such goods or services. A counterfeit mark is a mark that is used in connection with trafficking in goods or services, and is identical with, or substantially indistinguishable from a mark in use and registered for those goods or services on the principal register in the United States Patent and Trademark Office. It does not matter whether the defendant knew such mark was so registered. A counterfeit mark must also be one which is likely to cause confusion, to cause mistake, or to deceive.

You are instructed that it is not a defense that the counterfeit mark was modified in a trivial way, nor is it a defense that the defendant told the purchaser that the goods were counterfeit or that the counterfeit nature of the goods was apparent from the price. Thus, the test is whether an average consumer examining the goods would be deceived into believing that the product was made by the genuine trademark owner.

The evidence in this case includes of registration for [the good in question]. The certificate is Government's Exhibit No. _____. The certificate is prima facie evidence of the validity of the registered mark, of the ownership of the mark, and of owner's exclusive right to use the registered mark. "Prima facie evidence" means sufficient evidence to establish that the mark is valid, that the registrant owns the mark and has the exclusive right to use it.

Source: 18 U.S.C. § 2320

United States v. Torkington, 812 F.2d 1347, 1352 (11th Cir. 1987)

United States v. Gantos, 817 F.2d 41, 42 (8th Cir.), cert. denied, 484 U.S. 860
(1987)

United States v. Hon, 904 F.2d 803, 806 (2d Cir.), cert. denied, 498 U.S. 1069
(1991)

ELEMENTS OF THE OFFENSE KNOWLEDGE

The fourth element of trafficking in counterfeit goods or services is that the defendant knew that the mark used on or in connection with the trafficked goods or services was counterfeit. This means that the Government must show that the defendant was aware or had a firm belief of the counterfeit nature of the mark. The Government can meet this burden by proving that the defendant was willfully blind to the counterfeit nature of the mark. You are instructed that this showing can be made through circumstantial evidence regarding the purchase of the goods, the method of delivery, packaging conventions, and an unusually low price.

If you find that the defendant had a firm belief of the counterfeit nature of the mark, then you may find that the defendant knew that the mark was counterfeit.

Source: 18 U.S.C. § 2320

United States v. Sung, 51 F.3d 92, 94 (7th Cir.1995)

United States v. Jewell, 532 F.2d 697 (9th Cir.),
cert. denied, 426 U.S. 951 (1976)

United States v. Baker, 807 F.2d 427 (5th Cir. 1986)

**APPENDIX J: SAMPLE LANGUAGE FOR JURY INSTRUCTIONS -
18 U.S.C. § 1831**

**ECONOMIC ESPIONAGE
(18 U.S.C. § 1831)**

The defendant is charged in Count ____ of the indictment with economic espionage in violation of Section 1831 of Title 18 of the United States Code. In order for the defendant to be found guilty of this charge, the Government must prove each of the following elements beyond a reasonable doubt:

First, that the defendant stole or without the authorization of the owner [describe the misappropriation] information;

Second, that the defendant knew that the information was proprietary;

Third, that the information was in fact a trade secret; and

Fourth, that the defendant intended or knew that the misappropriation would benefit a foreign government, foreign instrumentality, or foreign agent.

ELEMENTS OF THE OFFENSE
MISAPPROPRIATION (18 U.S.C. § 1831(a)(1))

The first element of the offense is misappropriation. The Government must prove that the defendant knowingly stole, or without authorization appropriated, took, carried away, concealed, or by fraud, artifice or deception obtained information. You are instructed that authorization is the permission, approval, consent, or sanction of the owner to act.

If you find that the defendant stole, or without the permission, approval, consent, or sanction of the owner appropriated or obtained the information, then you may find that the defendant misappropriated the information without the consent of the owner.

Source: 18 U.S.C. § 1831(a)(1)

ELEMENTS OF THE OFFENSE
MISAPPROPRIATION (18 U.S.C. § 1831(a)(2))

The first element of the offense is misappropriation. The Government must prove that the defendant without authorization copied, duplicated, sketched, drew, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, or conveyed information. You are instructed that authorization is the permission, approval, consent, or sanction of the owner to act. You are also instructed that the Government does not have to prove that the defendant took the original property containing the information.

If you find that the defendant obtained, destroyed or conveyed the information without the authorization of the owner then you may find that the defendant misappropriated the information.

Source: 18 U.S.C. § 1831(a)(2)

ELEMENTS OF THE OFFENSE KNOWLEDGE

The second element of the offense charged is that the defendant knew or had a firm belief that the information he was misappropriating was proprietary. The Government must prove that the defendant was aware or substantially certain that the information he was appropriating was a trade secret.

If you find that the defendant had a firm belief that the information which he was appropriating was a trade secret, then you may find that the Government has proven this element.

Source: 18 U.S.C. 1831

ELEMENTS OF THE OFFENSE TRADE SECRET

The third element is that the [information in question] was a trade secret. With respect to this element of the offense charged, you are instructed that a trade secret includes all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored compiled, or memorialized physically, electronically, graphically, photographically, or in writing.

The Government must prove that the information was secret, that is, it was not generally known to the public. However, you are instructed that every part of the information need not be completely confidential to qualify as a trade secret. A trade secret can include a combination of elements that are in the public domain, if the trade secret constituted an effective, successful and valuable integration of public domain elements.

As part of this element, the Government must also prove that the owner of the trade secret took reasonable measures to keep the information secret. The Government does not have to prove that the security measures were absolute, but merely that such security measures were appropriate considering the value of the trade secret.

Finally, the Government must show that the trade secret derived actual or potential independent economic value from not being generally known to, and not being readily ascertainable through proper means by the public. You are instructed that where there is no

readily identifiable market for the trade secret, any reasonable method may be employed by the Government to show that the trade secret had economic value, including development, research and production costs.

If you find that the owner of the information took reasonable steps to keep the information secret, and that it derived independent economic value from not being known to, and not being readily ascertainable through proper means by the public, then you may find that the information was a trade secret.

Source: 18 U.S.C. § 1839

Rivendell Forest Prods. Ltd. v. Georgia-Pacific Corp., 28 F.3d 1042, 1046 (10th Cir. 1994)

Pioneer Hi-Bred Int'l v. Holden Found Seeds, 35 F.3d 1226, 1235 (8th Cir. 1994)

Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823, 828-49 (10th Cir. 1993)

United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988)

United States v. Drebin, 557 F.2d 1316, 1328 (9th Cir. 1977)

ELEMENTS OF THE OFFENSE
FOREIGN GOVERNMENT, FOREIGN INSTRUMENTALITY, FOREIGN AGENT

The fourth element of economic espionage is that the defense intended or knew that the offense would benefit a foreign government, foreign instrumentality or foreign agent. With respect to this element, you are instructed that benefit can be economic, reputational, strategic or tactical.

In the case of a foreign instrumentality, the Government must prove that the foreign instrumentality was substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government. You are instructed that, in such a case, the Government does not have to prove complete ownership, control, sponsorship, command, management or domination. The Government need only show that the activities of the foreign instrumentality are from a practical and substantive standpoint directed by a foreign government. You are also instructed that the term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government.

If you find that the defendant had a firm belief that the offense would benefit a foreign government, foreign instrumentality, or foreign agent, then you may find that the Government has proven this element.

Source: 18 U.S.C. §§ 1831, 1839

**APPENDIX K: SAMPLE LANGUAGE FOR JURY INSTRUCTIONS -
18 U.S.C. § 1832**

**THEFT OF TRADE SECRETS
(18 U.S.C. § 1832)**

The defendant is charged in Count ____ of the indictment with theft of trade secrets in violation of Section 1832 of Title 18 of the United States Code. In order for the defendant to be found guilty of this charge, the Government must prove each of the following elements beyond a reasonable doubt:

First, that the defendant stole or without the authorization of the owner, [describe the misappropriation] information;

Second, that the defendant knew that the information was proprietary;

Third, that the information was in fact a trade secret;

Fourth, that the defendant acted for the economic benefit of someone other than the owner of the trade secret;

Fifth, that the defendant intended or knew that the offense would injure the owner of the trade secret; and

Sixth, that the trade secret was related to or included in a product that is produced for or placed in interstate or foreign commerce.

ELEMENTS OF THE OFFENSE
MISAPPROPRIATION (18 U.S.C. § 1832(a)(1))

The first element of the offense is misappropriation. The Government must prove that the defendant knowingly stole, or without authorization appropriated, took, carried away, concealed, or by fraud, artifice or deception obtained information. You are instructed that authorization is the permission, approval, consent, or sanction of the owner to act. If you find that the defendant stole, or without the permission, approval, consent, or sanction of the owner appropriated or obtained the information, then you may find that the defendant misappropriated the information without the consent of the owner.

Source: 18 U.S.C. § 1832(a)(1)

ELEMENTS OF THE OFFENSE
MISAPPROPRIATION (18 U.S.C. § 1832(a)(2))

The first element of the offense is misappropriation. The Government must prove that the defendant without authorization copied, duplicated, sketched, drew, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, or conveyed information. You are instructed that authorization is the permission, approval, consent, or sanction of the owner to act. You are also instructed that the Government does not have to prove that the defendant deprived the owner of the physical property containing the information.

If you find that the defendant obtained, destroyed or conveyed the information without the authorization of the owner then you may find that the defendant misappropriated the information.

Source: 18 U.S.C. § 1832(a)(2)

ELEMENTS OF THE OFFENSE KNOWLEDGE

The second element of the offense charged is that the defendant knew or had a firm belief that the information he was taking was proprietary. The Government must prove that the defendant was aware or substantially certain that the information he was appropriating was a trade secret.

If you find that the defendant had a firm belief that the information which he was appropriating was a trade secret, then you may find that the Government has proven this element.

Source: 18 U.S.C. 1832

ELEMENTS OF THE OFFENSE TRADE SECRET

The third element is that the [information in question] was a trade secret. With respect to this element of the offense charged, you are instructed that a trade secret includes all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored compiled, or memorialized physically, electronically, graphically, photographically, or in writing.

The Government must prove that the information was secret, that is, it was not generally known to the public. However, you are instructed that every part of the information need not be completely confidential to qualify as a trade secret. A trade secret can include a combination of elements that are in the public domain, if the trade secret constituted an effective, successful and valuable integration of public domain elements.

As part of this element, the Government must also prove that the owner of the trade secret took reasonable measures to keep the information secret. The Government does not have to prove that the security measures were absolute, but merely that such security measures were appropriate considering the value of the trade secret.

Finally, the Government must show that the trade secret derived actual or potential independent economic value from not being generally known to, and not being readily ascertainable through proper means by the public. You are instructed that where there is no

readily ascertainable market for the trade secret, any reasonable method may be employed by the Government to show that the trade secret had economic value, including development, research and production costs.

If you find that the owner of the information took reasonable steps to keep the information secret, and that it derived independent economic value from not being known to, and not being readily ascertainable through proper means by the public, then you may find that the information was a trade secret.

Source: 18 U.S.C. § 1839

Rivendell Forest Prods. Ltd. v. Georgia-Pacific Corp., 28 F.3d 1042,
1046 (10th Cir. 1994)

Pioneer Hi-Bred Int'l v. Holden Found Seeds, 35 F.3d 1226,
1235 (8th Cir. 1994)

Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823,
828-49 (10th Cir. 1993)

United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988)

United States v. Drebin, 557 F.2d 1316, 1328 (9th Cir. 1977)

ELEMENTS OF THE OFFENSE ECONOMIC BENEFIT

The fourth element is that the defendant intended or knew that the offense would economically benefit a person (which can be the defendant or some other person or entity) other than the rightful owner .

If you find that the defendant committed the offense with the intent or knowledge that it would economically benefit a person other than the owner, then you may find that the Government has proven this element.

Source: 18 U.S.C. § 1832

ELEMENTS OF THE OFFENSE INJURY

The fifth element is that the defendant knew that the offense would injure any owner of the trade secret. You are instructed that the Government does not have to prove malice or evil intent. This means that the Government does not have to prove that the defendant acted with ill-will, but only that the defendant knew or was aware to a practical certainty that his conduct would cause some disadvantage to the owner.

If you find that the defendant knew that the offense would injure any owner of the trade secret, then you may find that the Government has proven this element.

Source: 18 U.S.C. § 1832

ELEMENTS OF THE OFFENSE INTERSTATE OR FOREIGN COMMERCE

The sixth and last element of the theft of trade secrets is that the Government must prove that the trade secret was related to or included in a product that was produced for or placed in interstate or foreign commerce. You are instructed that "produced" includes the research, development and manufacture of a product.

If you find that the trade secret was part of a product, in any stage of production, including research, development, and manufacture, and was for or placed in interstate or foreign commerce, then you may find that the trade secret was related to or included in a product that was produced for or placed in interstate or foreign commerce.

Source: 18 U.S.C. § 1832

APPENDIX L:**LIST OF STATES WITH "TRUE NAME AND ADDRESS" STATUTES**

ALABAMA	ALA CODE Secs. 13A-8-83 & 86
ALASKA *	ALASKA STAT. Sec. 45.50.900 (2)
ARIZONA	ARIZ. REV. STAT. Sec. 13-3705
ARKANSAS	ARK. STAT. ANN. Sec. 5-37 510(c)
CALIFORNIA	CAL. PENAL CODE Sec. 653(w)
COLORADO *	COLO. REV. STAT. Sec. 18-4-604
CONNECTICUT **	CONN. GEN. STAT. ANN. Sec. 53-142(c)
DELAWARE	DEL CODE ANN. Tit. 11, Sec. 922
FLORIDA	FLA. STAT. ANN. Sec. 540.11 (3)(a)
GEORGIA	GA. CODE ANN. Sec. 16-8-60(b)
IDAHO *	IDAHO CODE Secs. 18-7603(3), 18-7604
ILLINOIS	ILL. ANN. STAT. Ch.38, Sec. 16-8
INDIANA	IND. STAT. 24-4-10(4)
IOWA	IOWA CODE ANN. Sec.714.15
KANSAS	KAN. STAT. ANN. Sec.21-3750
KENTUCKY *	KY. REV. STAT. Sec.434.445(4)
LOUISIANA	LA.REV. STAT. ANN. Sec. 14:223.6
MARYLAND	MD. CRIM. LAW CODE ANN. Sec.467A(3)(b)
MASSACHUSETTS	MA. GEN. LAW ANN. Ch.226 Sec. 143c
MICHIGAN	MI.P.A. 210

MINNESOTA	MINN. STAT. ANN. Secs. 325E.18
MISSISSIPPI	MISS. CODE ABB. Sec. 97-23-89
MISSOURI	MO.ANN. STAT. Sec. 570.240-41
MONTANA *	MONT. CODE ANN. Sec. 30-13-144
NEBRASKA **	NEB. REV. STAT. Sec. 28-1324
NEVADA	NEV. REV. STAT. Sec. 205.217(2)
NEW HAMPSHIRE *	N.H. REV. STAT. ANN. Sec.352-A 3
NEW JERSEY	N.J.S. 2C:21:21c.(4)
NEW MEXICO	N.M. STAT. ANN. Sec.30-16B-4
NEW YORK	N.Y. PENAL LAW Sec.275.35 & 40
NORTH CAROLINA	N.C. GEN. STAT. Sec. 14-435
NORTH DAKOTA *	N.D. CENT. CODE. Sec.47-21. 1-03
OHIO ¹	OHIO REV. CODE ANN. Sec. 1333.52(B)
OKLAHOMA	OKLA. STAT. ANN.TITLE 21 Sec. 1979
OREGON	ORS 164.875 Sec. 8
PENNSYLVANIA *	PA. CONS. STAT. ANN. Tit. 18 Sec.4116(e)
RHODE ISLAND	R.I. GEN.LAWS Sec. 6-13.1-15(b)
SOUTH CARLOINA	S.C. CODE Sec. 16-11-930, 16-11-940
SOUTH DAKOTA	S.D. LAWS ANN. Sec.43-43A-3
TENNESSEE	TENN. CODE ANN. Sec. 39-14-139(a)
TEXAS	TEX. BUS. & COM. CODE Sec. 35.94
UTAH	UTAH CODE ANN. 1953, 13-10-8

VIRGINIA	VA. CODE Sec. 59.1-41.4
WASHINGTON	WASH. REV. CODE ANN. Sec. 19.25.040
WEST VIRGINIA *	W.VA. CODE Sec. 61-3-50

* Misdemeanor statute under which it may be necessary to purchase the pirated product to prove the violation.

** Misdemeanor statute.

APPENDIX M: State Criminal Trade Secret Statutes

The following states have statutes specifically providing criminal penalties for theft of trade secrets, or have general larceny statutes which make reference to theft of trade secrets. (Citations, unless otherwise indicated, refer to a specific trade secret criminal provision.)

Alabama	Al.St. § 13A-8-10.4
Arkansas	A.C.A § 5-36-107
California	Cal. Penal Code § 499(c)
Colorado	C.R.S.A. § 18-4-408
Connecticut	C.G.S.A. § 53a-124
Florida	F.S.A. § 812.081 (see also § 815.045, regarding computer-related trade secret theft)
Georgia	Code, 16-8-13
Idaho	Theft of trade secrets covered under general theft statute, I.C. § 18-2401
Illinois	Trade secret theft covered under general property crime statutes, 720 I.L.C.S. 5/15-1 et seq.
Indiana	Theft of trade secrets covered under general theft statutes, I.C. 35-43-1-4, 35-43-2-3
Louisiana	R.S. 14:73.2 ("Crime Against Intellectual Property")
Maine	17-A M.R.S.A. §§ 351-362
Maryland	Code 1957, Art. 27, §343; Code 1957, Art. 89, §§ 41-49A
Massachusetts	M.G.L.A. 266 § 30(4); see also M.G.L.A. 266 § 60A (prohibits buying of selling of stolen trade secrets)
Michigan	M.C.L.A. 752.772
Minnesota	M.S.A. § 609.52
Mississippi	Theft of trade secrets covered by general larceny statute, Code 1972, § 97-

	17-41; trade secret theft via computers also covered under computer crime statute, § 97-45-1 to 11
New Hampshire	R.S.A. 637:2, 637:3
New Jersey	Trade secret theft covered under general larceny statute, N.J.S.A. 2C:20-1 et seq.
New Mexico	Theft of trade secrets from employers covered by N.M.S.A. § 30-16-8 (embezzlement)
Ohio	Theft of trade secrets covered under general theft statute, § 2913.01.
Oklahoma	21 Okl.St. Ann. § 1732
Pennsylvania	18 Pa.C.S.A. § 3930
Tennessee	T.C.A. § 39-14-138
Texas	T.C.A. § 31.05
Wisconsin	W.S.A. § 943.205
Wyoming	Trade secret theft in general is covered by general larceny statute; "Crimes against intellectual property" via computers are prohibited under W.S.1977 § 6-3-502

APPENDIX N: LEGISLATIVE HISTORY - COPYRIGHT FELONY ACT

H.R. Rep. No. 997, 102ND Cong., 2ND Sess. 1992, 1992 U.S.C.C.A.N. 3569,

**P.L. 102-561, CRIMINAL PENALTIES FOR COPYRIGHT
INFRINGEMENT**

DATES OF CONSIDERATION AND PASSAGE

Senate: June 4, October 8, 1992

House: October 3, 1992

Senate Report (Judiciary Committee) No. 102-268,
Apr. 7, 1992 (To accompany S. 893)

House Report (Judiciary Committee) No. 102-997,
Oct. 3, 1992 (To accompany S. 893)

HOUSE REPORT NO. 102-997

October 3, 1992

[To accompany S. 893]

The Committee on the Judiciary, to whom was referred the Act (S. 893) to amend title 18, United States Code, to impose criminal sanctions for violation of software copyright, having considered the same, report favorably thereon with amendments and recommend that the Act as amended do pass.

The amendments are as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. CRIMINAL PENALTIES FOR COPYRIGHT INFRINGEMENT.

Section 2319(b) of title 18, United States Code, is amended to read as follows:

"(b) Any person who commits an offense under subsection (a) of this section-

"(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, with a retail value of more than \$2,500;

"(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

"(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case."

SEC. 2. CONFORMING AMENDMENTS.

Section 2319(c) of title 18, United States Code, is amended-

(1) in paragraph (1) by striking " 'sound recording', 'motion picture', audio-visual work', 'phonorecord'," and inserting " 'phonorecord' "; and

(2) in paragraph (2) by striking "118" and inserting "120". Amend the title so as to read: An Act to amend title 18, United States Code, with respect to the criminal penalties for copyright infringement.

EXPLANATION OF AMENDMENT

Inasmuch as S. 893 was ordered reported with a substitute to an amendment in the nature of a substitute, as amended, the contents of this report constitute an explanation of that substitute.

SUMMARY AND PURPOSE

The purpose of S. 893 is to harmonize the current felony provisions for copyright infringement and to provide an effective deterrence to the piracy of motion pictures, sound recordings, computer programs, and other original works of authorship. Piracy of copyrighted works costs U.S. industries millions of dollars a year, resulting in losses of jobs and diminution in the number of works created. Effective criminal penalties will aid in preventing Such losses.

INTRODUCTION

During this Congress, proposals to amend the copyright criminal felony provisions have been initiated by Senator Hatch, first as part of an omnibus crime package and later as a separate bill, S. 893. In both cases, the (identical) provisions concerned only computer programs. The provisions sought to amend title 18, United States Code, and built on amendments made in 1982 with respect to audiovisual works and sound recordings. There is no companion House bill.

The Subcommittee on Intellectual Property and Judicial Administration held a hearing on S. 893 on August 12, 1992. Testimony was received from: James Charne, General Counsel of Absolute Entertainment, Inc.; Gail Penner, Counsel, Autodesk, Inc. representing the Software Publishers Association; Edward J. Black, Vice President and General Counsel, Computer & Communications Industry Association; and, David Ostfeld, Chairman, Institute of Electrical & Electronics Engineers-U.S.A.

COMMITTEE VOTE

On September 30, 1992, a reporting quorum being present, the Committee ordered S. 893 reported to the full House by voice vote, with a substitute to an amendment in the nature of a substitute, as amended.

LEGISLATIVE HISTORY

S. 893 was introduced by Senator Hatch on April 23, 1991. Its provisions were also included as part of the omnibus crime package that passed the Senate on June 27, 1991. S. 893 was reported favorably by the Senate Committee on the Judiciary on April 7, 1992, [FN1] and passed the Senate, as amended, on June 4, 1992. The bill was referred to the Committee on the Judiciary on June 9, 1992, which, on June 11, 1992, referred the bill to the Subcommittee on Intellectual Property and Judicial Administration. On August 12, 1992, the Subcommittee held a hearing on S. 893, and on September 10, 1992 it marked-up and favorably approved an amendment in the nature of a substitute.

DISCUSSION

HISTORY OF CRIMINAL COPYRIGHT STATUTES

The first criminal provision in our copyright laws was a misdemeanor penalty added in 1897 for unlawful performances and representations of copyrighted dramatic and musical compositions. [FN2] In order to constitute a criminal violation, the defendant's conduct was required to have been "willful and for profit." Section 104 of the general copyright revision of 1909 extended this penalty to all types of copyrighted works, again if the conduct was done willfully and for profit. [FN3] Section 506(a) of the 1976 general Copyright Revision Act continued the misdemeanor provision [FN4] of the 1909 Act, but changed, without explanation, the phrasing of the mens rea requirement to conduct engaged in "willfully and for purposes of commercial advantage or private financial gain." Violators were to be fined not more than \$10,000 or imprisoned not more than 1 year, or both. In the case of sound recordings or motion pictures, violators were to be fined not more than \$25,000 or imprisoned for not more than 1 year, or both. [FN5] Repeat offenders were subject to a fine of not more than \$50,000 or imprisonment for not more than 2 years, or both.

In 1982, special provisions for motion pictures and sound recordings were added in the form of felony provisions for first time offenders. [FN6] This act amended both title 17 (the Copyright Act) and title 18. While the criminal offense remained in section 506(a) of title 17, the felony penalties for infringing reproductions or distributions of motion pictures or sound recordings were placed in new section 2319 of title 18, United States Code. [FN7]

As passed by the Senate, S. 893 sought to build on the 1982 amendments by including computer programs within the felony penalty provisions of section 2319 of title 18. [FN8]

AMENDMENTS

The substitute favorably reported by the Committee takes a different approach From S. 893 as passed by the Senate. Rather than simply adding computer programs to audiovisual works and sound recordings as works whose infringement can give rise to felony penalties, the substitute harmonizes the felony provisions in section 2319 to apply to all types of copyrighted works, as is currently the case for misdemeanor violations. The substitute does not alter the elements that must be established for a criminal copyright violation. The substitute also does not alter the misdemeanor provisions of the current law. Instead, the only changes made by the substitute are (1) an expansion in the types of copyrighted works that may give rise to felony prosecution, and, (2) a revision in the threshold that must be satisfied before felony liability may be imposed.

As in the past, whether conduct constitutes a criminal violation will be determined as follows. First, the Government is required to establish that an act or acts of copyright infringement have occurred. This *prima facie* case is determined by civil law. [FN9] Second, if a *prima facie* case of infringement is established, the Government must prove the defendant committed the infringement "willfully and for purposes of commercial advantage or private financial gain." [FN10] Third, if this *mens rea* is established, in order for the violation to be a felony, the infringing reproductions or distributions must meet certain numerical thresholds. Failure to meet those thresholds will result in the violation being treated as a misdemeanor.

Under the Committee substitute, the threshold for determining when an infringement accomplished with the requisite *mens rea* becomes a felony is to be determined through a combination of the number of infringing copies or phonorecords and their retail value. Specifically, at least 10 copies or phonorecords having a retail value of more than \$2,500 [FN11] must be reproduced or distributed without the copyright owner's permission within a 180 day period [FN12] in order to meet the thresholds.

MENS REA REQUIREMENT

The requirement of a *mens rea* for criminal copyright infringement serves the important purpose of drawing a sharp distinction with civil copyright infringement. Under civil copyright infringement, an intent to infringe is not required, since copyright is a strict liability tort. [FN13] For an infringement to be deemed a criminal violation, however, a specific *mens rea* must be proved. Even if civil liability has been established, without the requisite *mens rea* it does not matter how many unauthorized copies or phonorecords have been made or distributed: No criminal violation has occurred.

Under section 506(a) of title 17, United States Code, unamended by the substitute, the *mens rea* is described as infringement done "willfully and for purposes of commercial advantage or private financial gain." The term "willfully," although used in copyright statutes since 1897 for criminal violations, has never been defined. The substitute to S. 893 does not provide a definition either, since it is the Committee's intention that the standard as construed by the courts continue to be applied. [FN14]

The mens rea requirement serves to leave outside the reach of the criminal law losing parties in ordinary business disputes such as those involving reverse engineering of computer programs [FN15] or contract disputes over the scope of licenses. [FN16] Felony liability is not the result of every unauthorized reproduction or distribution of at least 10 copies or phonorecords having a retail value of more than \$2,500 within a 180-day period. First, infringement must be established. Next, the Government must prove that the infringement was done with the requisite mens rea. Unless both these requirements are met, no criminal liability-misdemeanor or felony-will lie, regardless of the number of unauthorized copies or phonorecords that have been reproduced or distributed. In cases where civil liability is unclear-whether because the law is unsettled, or because a legitimate business dispute exists- the Committee does not intend to establish criminal liability.

THE THRESHOLD REQUIREMENT OF NUMBER AND VALUE OF COPIES

The requirement that a requisite number of infringing copies or phonorecords be reproduced or distributed within a 180 day period serves a number of important purposes. First, it excludes from felony prosecution children making copies for friends as well as other incidental copying of copyrighted works having a relatively low retail value. Second, the requirement of reproducing or distributing at least 10 copies within a 180 day period removes the possibility that the increased penalties under the bill for computer program infringement can be used as a tool of harassment in business disputes over reverse engineering. Assuming arguendo that infringement due to unauthorized reverse engineering is established, and that the infringement was done with the requisite mens rea (which, as noted above, is unlikely), no felony liability should arise, since the Committee has been informed that reverse engineering does not require the reproduction of more than a handful of copies.

Where the requisite number of unauthorized copies or phonorecords with the requisite retail value have been made or distributed willfully and for purposes of commercial advantage or private financial gain within a 180 day period, the violator is subject to the following penalties: (1) imprisonment of not more than 5 years and/or the fine prescribed in title 18 for a first offense; [FN17] (2) imprisonment of not more than 10 years and/or the fine prescribed in title 18 for a second or subsequent offense.

SECTION-BY-SECTION ANALYSIS OF THE COMMITTEE SUBSTITUTE

SECTION 1

Section 1 of the Committee substitute amends section 2319(b) of title 18 in its entirety. Under the substitute, any person who violates section 506(a) of title 17, United States Code, shall be imprisoned for not more than 5 years, or fined in the amount set forth in title 18, or both, if the offense consists of the reproduction or distribution of at least 10 copies or phonorecords, of one or more copyrighted works, with a retail value of more than \$2,500 during a 180 day period. [FN18]

The phrase "of one or more copyrighted works" is intended to permit aggregation of

different works of authorship to meet the required number of copies and retail value. For example, a defendant's reproduction of 5 copies of a copyrighted word processing computer program having a retail value of \$1,300 and the reproduction of 5 copies of a copyrighted spreadsheet computer program also having a retail value of \$1,300 would satisfy the requirement of reproducing 10 copies having a retail value of at least \$2,500, if done within a 180 day period.

The term "retail value" is deliberately undefined, since in most cases it will represent the price at which the work is sold through normal retail channels. [FN19] At the same time, the Committee recognizes that copyrighted works are frequently infringed before a retail value has been established, and that in some cases, copyrighted works are not marketed through normal retail channels. Examples include motion pictures prints distributed only for theatrical release, and beta-test versions of computer programs. In such cases, the courts may look to the suggested retail price, the wholesale price, the replacement cost of the item, or financial injury caused to the copyright owner.

If the offense is a second or subsequent offense, the defendant is subject to imprisonment for not more than 10 years, or a fine in the amount set forth in title 18, United States Code, or both.

If the defendant failed to make the requisite number or value of copies within the 180 day period, but still engaged in the infringing conduct with the requisite mens rea, section 2319(b)(3) subjects the defendant to a term of imprisonment of not more than 1 year or a fine in the amount set forth in title 18, United States Code, or both, as under current law.

SECTION 2

Section 2 contains conforming amendments. Since the substitute harmonizes the felony penalties to apply to all types of copyrighted works, section 2 deletes the references to "sound recording," "motion picture" and "audiovisual work."

EFFECTIVE DATE

The substitute shall take effect on the date of enactment and applies only to conduct engaged in on or after that date.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 2(l)(3)(A) of rule XI of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

COMMITTEE ON GOVERNMENT OPERATIONS OVERSIGHT FINDINGS

No findings or recommendations of the Committee on Government Operations were received as referred to in clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 2(l)(3)(B) of House Rule XI is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 2(l)(3)(C) of rule XI of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill S. 893, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 403 of the Congressional Budget Act of 1974:

U.S. Congress,
Congressional Budget Office,
Washington, DC, October 2, 1992.
Hon. Jack Brooks,
Chairman, Committee on the Judiciary,
House of Representatives, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has reviewed S. 893, a bill to amend title 18, United States Code, to impose criminal sanctions for violation of software copyright, as ordered reported by the House Committee on the Judiciary on September 30, 1992. Enactment of this bill would increase costs to the federal government because prison terms served by some copyright offenders would be longer. It also could increase receipts to the federal government from fines, but we cannot estimate the amount of either increase.

Because S. 893 could affect receipts, it would be subject to pay-as-you-go procedures under section 252 of the Balanced Budget and Emergency Deficit Control Act of 1985. Therefore, the estimate required under clause 8 of House Rule XXI is attached.

Under current law, only certain offenses involving copyright violations of sound recordings or audiovisual works are felonies, while all other copyright violations are misdemeanors. S. 893 would change the criteria for determining whether a copyright violation involving sound recordings or audiovisual works is a felony offense. In addition, the bill would apply the same criteria to all copyright violations, not just those involving sound recordings or audiovisual works.

It is impossible to predict with confidence the effect of the new criteria for determining felonies, because some copyright violations that otherwise would have been felony offenses would be misdemeanor offenses, and vice versa. Some offenses that could only have been

misdemeanors-namely, those not involving sound recordings or audiovisual works-would be felonies under S. 893.

This probably would result in increased prison terms served and/or fines paid by these offenders, but CBO has no basis for quantifying the increased cost or receipts to the federal government. Any such costs would be paid from appropriated funds.

CBO estimates that enactment of S. 893 would result in no cost to state or local governments.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz, and John Stell.

Sincerely,
James L. Blum
(For Robert D. Reischauer, Director).

CONGRESSIONAL BUDGET OFFICE ESTIMATE [FN1]

The applicable cost estimate of this act for all purposes of sections 252 and 253 of the Balanced Budget and Emergency Deficit Control Act of 1985 shall be as follows.

TABULAR OR GRAPHIC MATERIAL SET FORTH AT THIS POINT IS NOT
DISPLAYABLE

INFLATIONARY IMPACT STATEMENT

Pursuant to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the Committee estimates that S. 893 will have no significant impact on prices and costs in the national economy.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

SECTION 2319 OF TITLE 18, UNITED STATES CODE

* * * * *

S 2319. Criminal infringement of a copyright

(a) * * *

(b) Any person who commits an offense under subsection (a) of this section-

- (1) shall be fined not more than \$250,000 or imprisoned for not more than five years, or both, if the offense-
- (A) involves the reproduction or distribution, during any one-hundred-and-eighty-day period, of at least one thousand phonorecords or copies infringing the copyright in one or more sound recordings;
 - (B) involves the reproduction or distribution, during any one-hundred-and-eighty-day period, of at least sixty-five copies infringing the copyright in one or more motion pictures or other audiovisual works; or
 - (C) is a second or subsequent offense under either of subsection (b)(1) or (b)(2) of this section, where a prior offense involved a sound recording, or a motion picture or other audiovisual work;
- (2) shall be fined not more than \$250,000 or imprisoned for not more than two years, or both, if the offense-
- (A) involves the reproduction or distribution, during any one-hundred-and-eighty-day period, of more than one hundred but less than one thousand phonorecords or copies infringing the copyright in one or more sound recordings; or
 - (B) involves the reproduction or distribution, during any one-hundred-and-eighty-day period, of more than seven but less than sixty-five copies infringing the copyright in one or more motion pictures or other audiovisual works; and
- (3) shall be fined not more than \$25,000 or imprisoned for not more than one year, or both, in any other case.)
- (b) Any person who commits an offense under subsection (a) of this section-
- (1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, with a retail value of more than \$2,500;
 - (2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
 - (3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.
- (c) As used in this section-
- (1) the terms ("sound recording", "motion picture", "audiovisual work", "phonorecord",) "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and
 - (2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through (118,) 120, of title 17.

FN1 S. Rept. No. 102-268, 102d Cong., 2d Sess.

FN2 Act of January 6, 1897, 54th Cong., 2d Sess., 29 Stat. 481.

FN3 This provision also imposed liability on those who "knowingly and willfully" aided and abetted criminal infringement.

FN4 The 1976 act dropped the aiding and abetting provision of the former law, however.

FN5 For sound recordings, criminal infringement would lie for violation of the reproduction, derivative, or distribution rights. For motion pictures, criminal infringement would lie for infringement of the reproduction, distribution, or public performance rights. 17 U.S.C. S 506(a)(1978).

FN6 Act of May 24, 1982, P.L. 97-180, 97th Cong., 2d Sess., 96 Stat. 91.

FN7 Section 2319 of title 18 currently reads:

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsection (b) of this section and such penalties shall be in addition to any other provision of title 17 or any other law.

(b) Any person who commits an offense under subsection (a) of this section-

(1) shall be fined not more than \$250,000 or imprisoned for not more than 5 years, or both, if the offense-

(A) involves the reproduction or distribution, during any 180-day period, of at least 1,000 phonorecords or copies infringing the copyright in one or more sound recordings;

(B) involves the reproduction or distribution, during any 180-day period, of at least 65 copies infringing the copyright in one or more motion pictures or other audiovisual works; or

(C) is a second or subsequent offense under either of subsection (b)(1) or (b)(2) of this section, where a prior offense involved a sound recording, or a motion picture or other audiovisual work;

(2) shall be fined not more than \$250,000 or imprisoned for not more than 2 years, or both, if the offense-

(A) involves the reproduction or distribution, during any 180-day period, of more than 100 but less than 1,000 phonorecords or copies infringing the copyright in one or more sound recordings; or

(B) involves the reproduction or distribution, during any 180-day period, of more than 7 but less than 65 copies infringing the copyright in one or more motion pictures or other audiovisual works; and

(3) shall be fined not more than \$25,000 or imprisoned for not more than 1 year, or both, in any other case.

FN8 Specifically, S. 893 as passed by the Senate provided for:

(1) A fine of not more than \$250,000 or imprisonment for not more than 5 years or both if, during any 180-day period, at least 50 copies infringing the copyright in one or more computer programs are reproduced or distributed;

(2) A fine of not more than \$250,000 or imprisonment for not more than 2 years or both if, during any 180-day period, more than 10 but less than 50 copies infringing the copyright in one or more computer programs are reproduced or distributed.

(3) A second or subsequent offender under either (1) or (2) will be punished under (1).

FN9 *United States v. Larracuente*, 952 F.2d 673, 673 (2d Cir. 1992); *United States v. Cross*, 816 F.2d 297, 303 (7th Cir. 1987); *United States v. O'Reilly*, 230 USPQ 475 (11th Cir. 1986).

FN10 17 U.S.C. S 506(a) (1978).

FN11 As under current law, the felony penalties are only for violations of the reproduction or distribution right; infringement of the right to prepare derivative works, the right to publicly perform a copyrighted work, or the right to publicly display a copyrighted work is subject only to a misdemeanor penalty.

FN12 This one hundred and eighty day provision was added as an amendment by Mr. Campbell, and conforms to the current provisions in section 2319 of title 18, United States Code.

FN13 *Buck v. Jewell-LaSalle Realty Co.*, 283 U.S. 191, 198 (1931).

FN14 See e.g., *United States v. Cross*, 816 F.2d 297, 300 (7th Cir. 1987) (defendant must have engaged in the infringing conduct with knowledge that his or her activity was prohibited by law.) For decisions under the 1909 Act, see *United States v. Backer*, 134 F.2d 533 (2d Cir. 1943), and *United States v. Taxe*, 540 F.2d 961 (9th Cir. 1976), cert denied, 429 U.S. 1040 (1977). In *Backer*, the Second Circuit found liability where the defendant, although without actual notice from the copyright owner, unlawfully issued instructions to make copies resembling the copyrighted work "as closely as they might without 'copyright trouble,'" indicating that the defendant was aware of the legal prohibition against infringement. In *Taxe*, the 9th Circuit affirmed a jury instruction that advice of counsel is "no defense" but should be considered in whether the defendant's action was "willful."

FN15 This legislation should not be construed by the courts as expressing Congressional intent on the question of whether reverse engineering is or is not a civil violation of copyright law. S. 893 is an amendment the criminal copyright law provisions, and assumes that a prima facie case of infringement has been proven. The elements of the civil offense of infringement are left to the developing jurisprudence in the area.

FN16 See *United States v. Larracuente*, 952 F.2d 672, 673 -674 (2d Cir. 1992) ("If the accused infringer has been licensed by a licensee of the copyright owner, that is a matter of affirmative

defense").

FN17 See 18 U.S.C. S 3571(b) (fines for individuals); *id.*, S 3571(c) (fines for organizations).

FN18 This 180 day period does not change the 3 year statute of limitations period set forth in section 507(a).

FN19 See generally, *United States v. Larracuente*, 952 F.2d 672, 674 (2d Cir.1992) (holding that trial court was correct in applying the Sentencing Commission's guidelines "to the normal retail price, rather than the lower bootleg price paid by those who presumably are aware that the prices they are buying are not legitimate," but noting possible exceptions).

FN1 An estimate of S. 893 as ordered reported by the House Committee on the Judiciary on September 30, 1992. This estimate was transmitted by the Congressional Budget Office on October 2, 1992.

H.R. REP. 102-997, H.R. Rep. No. 997, 102ND Cong., 2ND Sess. 1992,
1992 U.S.C.C.A.N. 3569.

**APPENDIX O: LEGISLATIVE HISTORY - ECONOMIC ESPIONAGE ACT OF
1996**

Congressional Record --- Senate
Proceedings and Debates of the 104th Congress, Second Session
Wednesday, October 2, 1996

***S12201 ECONOMIC ESPIONAGE ACT OF 1996**

Mr. NICKLES.

Mr. President, I ask the Chair to lay before the Senate a message from the House of Representatives on (H.R. 3723) the bill to amend title 18, United States Code, to protect proprietary economic information, and for other purposes.

The PRESIDING OFFICER laid before the Senate the following message from the House of Representatives:

Resolved, That the House agree to the amendment of the Senate to the bill (H.R. 3723) entitled "An Act to amend title 18, United States Code, to protect proprietary economic information, and for other purposes", with the following House amendment to senate amendment:

In lieu of the matter proposed to be inserted by the Senate amendment to the text of the bill, insert:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Economic Espionage Act of 1996".

TITLE I-PROTECTION OF TRADE SECRETS

SEC. 101. PROTECTION OF TRADE SECRETS.

(a) IN GENERAL.-Title 18, United States Code, is amended by inserting after chapter 89 the following:

"CHAPTER 90-PROTECTION OF TRADE SECRETS

"Sec.

"1831. Economic espionage.

"1832. Theft of trade secrets.

"1833. Exceptions to prohibitions.

"1834. Criminal forfeiture.

"1835. Orders to preserve confidentiality.

"1836. Civil proceedings to enjoin violations.

"1837. Conduct outside the United States.

"1838. Construction with other laws.

"1839. Definitions.

"§ 1831. Economic espionage

"(a) IN GENERAL.-Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly-

"(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

"(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

"(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

"(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

"(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (4), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than \$500,000 or imprisoned not more than 15 years, or both.

"(b) ORGANIZATIONS.-Any organization that commits any offense described in subsection (a) shall be fined not more than \$10,000,000.

"s1832. Theft of trade secrets

"(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly-

"(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

"(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

"(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

"(4) attempts to commit any offense described in paragraphs (1) through (3); or

"(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

"(b) Any organization that commits any offense described in subsection (a) shall be fined not more than \$5,000,000.

"§ 1833. Exceptions to prohibitions

"This chapter does not prohibit-

"(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

"(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

"§ 1834. Criminal forfeiture

"(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States-

"(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

"(2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

"(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section, which shall not apply to forfeitures under this

section.

"§ 1835. Orders to preserve confidentiality

"In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

"§ 1836. Civil proceedings to enjoin violations

"(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

"(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

"§ 1837. Applicability to conduct outside the United States

"This chapter also applies to conduct occurring outside the United States if-

"(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or

*S12202 "(2) an act in furtherance of the offense was committed in the United States.

"§ 1838. Construction with other laws

"This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

"§ 1839. Definitions

"As used in this chapter-

"(1) the term 'foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

"(2) the term 'foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

"(3) the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if-

"(A) the owner thereof has taken reasonable measures to keep such information secret; and

"(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

"(4) the term 'owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed."

(b) CLERICAL AMENDMENT.-The table of chapters at the beginning part I of title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following:

(c) REPORTS.-Not later than 2 years and 4 years after the date of the enactment of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims Fund established by section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601).

"90. Protection of trade secrets1831

Mr. SPECTER.

Mr. President, I am pleased that the Senate is acting today to pass the Economic Espionage Act of 1996, legislation Senator KOHL and I introduced earlier this year to combat economic espionage. This bill addresses an issue of critical importance to our Nation's economic well-being. It is a testament to the importance of the issue that we are able to act in a bipartisan

fashion on the eve of national elections.

As chairman of both the Select Committee on Intelligence and the Judiciary Committee's Subcommittee on Terrorism, Technology and Government Information, with jurisdiction over legal matters involving technology, I have been concerned with the threat posed to American economic competitiveness in a global economy by the theft of intellectual property and trade secrets.

In an increasingly complex and competitive economic world, intellectual property forms a critical component of our economy. As traditional industries shift to low-wage producers in developing countries, our economic edge depends to an ever-increasing degree on the ability of our businesses and inventors to stay one step ahead of those in other countries. And American business and inventors have been extremely successful and creative in developing intellectual property and trade secrets. America leads the nation's of the world in developing new products and new technologies. Millions of jobs depend on the continuation of the productive minds of Americans, both native born and immigrants who find the freedom here to try new ideas and add to our economic strength.

Inventing new and better technologies, production methods, and the like, can be expensive. American companies and the U.S. Government spend (*\$12207) billions on research and development. The benefits reaped from these expenditures can easily come to nothing, however, if a competitor can simply steal *\$12208 the trade secret without expending the development costs. While prices may be reduced, ultimately the incentives for new invention disappear, along with jobs, capital investment, and everything else that keeps our economy strong.

For years now, there has been mounting evidence that many foreign nations and their corporations have been seeking to gain competitive advantage by stealing the trade secrets, the intangible intellectual property of inventors in this country. The Intelligence Committee has been aware that since the end of the cold war, foreign nations have increasingly put their espionage resources to work trying to steal American economic secrets. Estimates of the loss to U.S. business from the theft of intangible intellectual property exceed \$100 billion. The loss in U.S. jobs is incalculable.

For the benefit of my colleagues who wish more detail about the nature and scope of the problem of economic espionage, I ask unanimous consent that a copy of the article "The Lure of the Steal" from the March 4, 1996, U.S. News & World Report, and an article by Peter Schweizer, "The Growth of Economic Espionage-America if Target Number One" from the January-February 1996 edition of Foreign Affairs be printed at the end of my remarks.

The PRESIDING OFFICER.

Without objection, it is so ordered.

(See exhibit 1)

Mr. SPECTER.

Mr. President, a major problem for law enforcement in responding to the increase in such thefts has been a glaring gap in Federal law. For many years, the United States has had a variety

of theft statutes in the United States Code. These laws are derived primarily from the common law of theft. For example, it violates Federal law to move stolen property across State lines. In order to violate such laws, however, the courts have held that the property stolen cannot be intangible property, such as trade secrets or intellectual property. In addition, theft usually requires that the thief take the property with the intention of depriving the lawful owner of its use. But such a test is useless when a person copies software and leaves the original software with the lawful owner, taking only the secrets on the software but leaving the physical property. The lawful owner still has full use of the property, but its value is significantly reduced.

In order to update Federal law to address the technological and economic realities of the end of the 20th century, I began working earlier this year with Senator KOHL and officials from the Department of Justice and the Federal Bureau of Investigation on developing legislation. We developed two separate bills, that were introduced as S. 1556 and S. 1557. The former bill broadly prohibited the theft of proprietary economic information by any person. The latter bill was more narrowly drawn to proscribe such thefts by foreign nations and those working on behalf of foreign nations.

At the end of February, I chaired a joint hearing of the Intelligence Committee and the Judiciary Subcommittee on Terrorism, Technology, and Government Information on the issue of economic espionage. Continuing to work closely with members of the Judiciary and Intelligence Committees, the administration, and various industry groups, Senator KOHL and I were able to produce the bill the Senate is today considering.

The Senate adopted S. 1556 with an amendment I offered, based on S. 1557, to bring together into a single vehicle the prohibition on the theft of trade secrets and proprietary information by both private individuals and corporations and by foreign governments and those acting on their behalf, and passed them using H.R. 3723, the House companion bill, as the vehicle. The language of my amendment dealing with foreign-government-sponsored economic espionage was, with minor changes, unanimously reported to the Senate by the Intelligence Committee earlier this year as part of the Intelligence Authorization Act. We have now reconciled the Senate and House-passed bills in this agreement, which also incorporates several unrelated provisions. Senator KOHL and I are inserting into the RECORD a managers' statement which reflects the understanding of the bill's sponsors on the intent behind and meaning of the economic espionage bill.

Adoption of this bill will not be a panacea, but it is a start. Congress has started moving to protect U.S. economic interests. For example, earlier this year we enacted strong anticounterfeiting legislation, S. 1136, to protect American business from counterfeit goods. This bill addresses cognate problems. Both are only a start. Corporations must exercise vigilance over their trade secrets and proprietary information. Contract law may provide civil remedies. In addition, some States have adopted legislation to allow the owners of trade secrets to use civil process to protect their ownership rights. We have been made aware that available civil remedies may not be adequate to the task and that a Federal civil cause of action is needed. This is an issue we need to study carefully, and will do so next year.

For helping to make sure that this legislation was passed this year, I want to thank Senator KOHL for his leadership, and acknowledge the work of his excellent staff, Jon Leibowitz and Victoria Bassetti. I also want to thank the chairman of the Judiciary Committee, Senator

HATCH, and his staff, especially Paul Larkin and Pat Murphy, for their valuable contributions to this legislation. I would also be remiss if I did not also thank Chairman MCCOLLUM of the House Crime Subcommittee, and Representative SCHUMER, ranking member of that Subcommittee, and their staff, Glenn Schmitt and Bill McGeeveran, for their hard work. Finally, we worked closely with the Justice Department and the Federal Bureau of Investigation in developing this legislation, and I want to thank Alan Hoffman of the Justice Department and Pat Kelly of the FBI for their hard work on this bill.

*S12211

Mr. KOHL.

Mr. President, today, we pass the Economic Espionage Act, which is based upon legislation drafted by Senator SPECTER and me and, on the House side, by Representatives MCCOLLUM and SCHUMER. In a Congress marked by so much partisanship, this legislation marks a significant bipartisan accomplishment. With this new law, we penalize the theft of vital economic information.

Since the end of the cold war, our old enemies and our traditional allies have been shifting the focus of their spy apparatus. Alarming, the new target of foreign espionage is our industrial base. But for too many years, we were complacent and did not heed these warnings. And we left ourselves vulnerable to the ruthless plundering of our country's vital information. We did not address this new form of espionage-a version of spying as dangerous to our national well-being as any form of classic espionage. Today, that complacency ends.

Mr. President, this legislation is crucial. Most Americans probably do not realize that anyone with the wherewithal to do it can walk out of a company with a computer disk full of its most important manufacturing information and sell that information to the highest bidder with virtual impunity-and no criminal penalties.

This problem is even worse when foreign governments have specifically focussed on American companies in order to steal information from them. American companies are not prepared or equipped to fight off this kind of systematic targeting.

The executive vice president of Corning, James Riesbeck, has said that:

It is important to understand that State-sponsored industrial espionage is occurring in the international business community. It is very difficult for an individual corporation to counteract this activity. The resources of any corporation are no match for industrial espionage that is sanctioned and supported by foreign governments.

A report of the National Counterintelligence Center <NCIC> in 1995 indicated that biotechnology, aerospace, telecommunications, computer software, transportation, advanced materials, energy research, defense, and semiconductor companies are all top targets for foreign economic espionage. These sectors are aggressively targeted according to the report. That report identified 20 different methods used to conduct industrial espionage. The traditional methods include recruiting an agent and then inserting the agent into the target company, or breaking into an office to take equipment and information. According to the report, computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses account

for the largest portion of economic and *S12212 industrial information lost by U.S. corporations.

But even as American companies are attempting to respond to foreign espionage, they also have to address theft by insiders. A survey by the American Society for Industrial Security <ASIS> of 325 companies in 1995 found that almost half of them had experienced trade secret theft of some sort during the previous 2 years. They also reported a 323-percent increase in the number of incidents of intellectual property loss. A 1988 National Institute of Justice study of trade secret theft in high-technology industries found that 48 percent of 150 research and development companies surveyed had been the victims of trade secrets theft. Almost half of the time the target was research and development data while 38 percent of the time the target was new technology. Forty percent of the victims found out about the theft from their competitors.

Norman Augustine, the president of Lockheed Martin Corp., told us at our February hearings that a recent survey of aerospace companies revealed that 100 percent of them believe that a competitor, either domestic or international, has used intelligence techniques against them.

And, Mr. President, make no mistake about it, economic espionage costs our country dearly. In 1992, when a representative of IBM testified at a House hearing on this issue, he told us that economic espionage had cost his company billions of dollars. The NCIC report concluded that industry victims have reported the loss of hundreds of millions of dollars, lost jobs, and lost market share. The ASIS survey concluded that the potential losses could total \$63 billion a year.

Because of the gap in our laws, Senator SPECTER and I introduced two companion measures that became the Economic Espionage Act earlier this year. This legislation will be used to go after the foreign intelligence services that take aim at American companies and at the people who walk out of businesses with millions of dollars worth of information.

I will only briefly explain what we have done here because the managers' statement and the House and Senate committee reports fully and completely describe this act. This legislation makes it illegal to steal trade secrets from companies. It enhances the penalties when the theft is at the behest of a foreign government. With the help of Senator HATCH and Representatives MCCOLLUM and SCHUMER, we have carefully drafted these measures to ensure that they can only be used in flagrant and egregious cases of information theft. Moreover, trade secrets are carefully defined so that the general knowledge and experience that a person gains from working at a job is not covered.

Mr. President, we do not want this law used to stifle the free flow of information or of people from job to job. But we built in a number of safeguards to prevent exactly these problems. They are elaborated on in the managers' statement and our committee reports.

Mr. President, I ask unanimous consent that a copy of the managers' statement be printed in the RECORD. It reflects our understanding on this measure.

There being no objection, the managers' statement was ordered to be printed in the RECORD, as follows:

MANAGERS' STATEMENT FOR H.R. 3723, THE ECONOMIC ESPIONAGE BILL

This legislation is based upon two bills, S. 1556, "The Industrial Espionage Act of 1996,"

and S. 1557, "The Economic Security Act of 1996," which were introduced by Senators SPECTER and KOHL. This Managers' Statement is intended to clarify portions of the legislation and to supplement the Committee reports already issued on these two measures. It also explains how the House and Senate version of the legislation were reconciled.

DIFFERENCE BETWEEN SECTIONS 1831 AND 1832

This legislation includes a provision penalizing the theft trade secrets (Sec. 1832) and a second provision penalizing that theft when it is done to benefit a foreign government, instrumentality, or agent (Sec. 1831). The principle purpose of this second (foreign government) provision is not to punish conventional commercial theft and misappropriation of trade secrets (which is covered by the first provision). Thus, to make out an offense under the economic espionage section, the prosecution must show in each instance that the perpetrator intended to or knew that his or her actions would aid a foreign government, instrumentality, or agent. Enforcement agencies should administer this section with its principle purpose in mind and therefore should not apply section 1831 to foreign corporations when there is no evidence of foreign government sponsored or coordinated intelligence activity.

This particular concern is borne out in our understanding of the definition of "foreign instrumentality" which indicates that a foreign organization must be "substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government or subdivision thereof." Although the term "substantially" is not specifically defined, it is a relative term that connotes less than total or complete ownership, control, sponsorship, command, management, or domination. Substantial in this context, means material or significant, not technical or tenuous. We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns 10 percent of a company exempt it from scrutiny. Rather the pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.

To make out a case under these two provisions (sections 1831 and 1832), the prosecution would have to show that the accused knew or had reason to know that a trade secret had been stolen or appropriated without authorization. This threshold separates conduct that is criminal from that which is innocent. Thus, for example, these sections would not give rise to a prosecution for legitimate economic collection or reporting by personnel of foreign governments or international financial institutions, such as the World Bank, because such legitimate collection or reporting would not include the collection or reporting of trade secrets that had been stolen, misappropriated or converted without authorization.

WITHOUT AUTHORIZATION

Several federal statutes already include the requirement that information be taken "without authorization." The most notable is 18 U.S.C. §1030, which is amended in this measure by the National Information Infrastructure Protection Act introduced by Senators Leahy, Kyl and

Grassley. That provision essentially deals with authorization in relation to computer systems. However, in this legislation the nature of authorization may be slightly different since this measure involves information "whether or how stored." But the principle remains the same: authorization is the permission, approval, consent, or sanction of the owner.

PARALLEL DEVELOPMENT NOT COVERED

It is important to note that a person who develops a trade secret is not given an absolute monopoly on the information or data that comprises a trade secret. For example, if a company discovers that a particular manufacturing process must be conducted at a certain ambient temperature and that a more than 10 percent deviation from that temperature will compromise the process, that company does not have the exclusive right to manufacture the product at the key temperature (assuming that this is not otherwise patented or protected by law). Other companies can and must have the ability to determine the elements of a trade secret through their own inventiveness, creativity and hard work. As the Supreme Court noted in *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974): "If something is to be discovered at all very likely it will be discovered by more than one person. . . . Even were an inventor to keep his discovery completely to himself, something that neither the patent nor trade secret laws forbid, there is a high probability that it will be soon independently developed. If the invention, though still a trade secret, is put into public use, the competition is alerted to the existence of the inventor's solution to the problem and may be encouraged to make an extra effort to independently find the solution this known to be possible." *Id.* at 490-91.

This legislation does not in any way prohibit companies, manufacturers, or inventors from using their skills, knowledge and experience to solve a problem or invent a product that they know someone else is also working on. Thus, parallel development of a trade secret cannot and should not constitute a violation of this statute. This includes the situation in which an individual inventor, unsolicited, sends his or her material to a manufacturer even as the company itself is in the midst of its own parallel development. In the first place, this wholesale disclosure of material likely breaches the requirement that a trade secret owner take reasonable measures to protect the information's confidentiality. But more importantly, many companies regularly receive such ideas and inventions and do not use them. Some of these unsolicited ideas and inventions may overlap with work being done within the company already. Both the individual inventor and the company are conducting parallel work, pursuing the same line of inquiry. Neither can be subject to penalty under this law.

REVERSE ENGINEERING

Some people have asked how this legislation might affect reverse engineering. Reverse engineering is a broad term that encompasses a variety of actions. The important thing is to focus on whether the accused has committed one of the prohibited acts of *S12213 this statute rather than whether he or she has "reverse engineered." If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent or this law, then that form of "reverse engineering" should be fine. For example, if a person can drink Coca-Cola and,

because he happens to have highly refined taste buds, can figure out what the formula is, then this legislation cannot be used against him. Likewise, if a person can look at a product and, by using their own general skills and expertise, dissect the necessary attributes of the product, then that person should be free from any threat of prosecution.

DEFINITION OF TRADE SECRETS

Unlike patented material, something does not have to be novel or inventive, in the patent law sense, in order to be a trade secret. Of course, often it will be because an owner will have a patented invention that he or she has chosen to maintain the material as a trade secret rather than reveal it through the patent process. Even if the material is not novel in the patent law sense, some form of novelty is probably inevitable since "that which does not possess novelty is usually known; secrecy, in the context of trade secrets implies at least minimal novelty." *Kewanee Oil Co.*, 416 U.S. at 476. While we do not strictly impose a novelty or inventiveness requirement in order for material to be considered a trade secret, looking at the novelty or uniqueness of a piece of information or knowledge should inform courts in determining whether something is a matter of general knowledge, skill or experience.

Although we do not require novelty or inventiveness, the definition of a trade secret includes the provision that an owner have taken reasonable measures under the circumstances to keep the information confidential. We do not with this definition impose any requirements on companies or owners. Each owner must assess the value of the material it seeks to protect, the extent of a threat of theft, and the ease of theft in determining how extensive their protective measures should be. We anticipate that what constitutes reasonable measures in one particular field of knowledge or industry may vary significantly from what is reasonable in another field or industry. However, some common sense measures are likely to be common across the board. For example, it is only natural that an owner would restrict access to a trade secret to the people who actually need to use the information. It is only natural also that an owner clearly indicate in some form or another that the information is proprietary. However, owners need not take heroic or extreme measures in order for their efforts to be reasonable.

GENERAL KNOWLEDGE NOT COVERED BY DEFINITION OF TRADE SECRETS

In the course of reconciling the Senate and House versions of this legislation, we eliminated the portion of the definition of trade secret that indicated that general knowledge, skills and experience were not included in the meaning of that term. Its elimination from the statutory language does not mean that general knowledge can be a trade secret. Rather, we believed that the definition of trade secrets in itself cannot include general knowledge. Thus, it was unnecessary and redundant to both define what does and what does not constitute a trade secret.

Our reason initially for putting the exception in was to state as clearly as possible that this legislation does not apply to innocent innovators or to individuals who seek to capitalize on

their lawfully developed knowledge skill or abilities. Employees, for example, who change employers or start their own companies should be able to apply their talents without fear of prosecution because two safeguards against overreaching are built into the law.

First, protection is provided by the definition of "trade secret" itself. The definition requires that an owner take objectively reasonable, proactive measures, under the circumstances, to protect the information. If, consequently, an owner fails to safeguard his or her trade secret, then no one could be rightfully accused of misappropriating it. Most owners do take reasonable measures to protect their trade secrets, thereby placing employees and others on clear notice of the discreet, proprietary nature of the information.

In addition, a prosecution under this statute must establish a particular piece of information that a person has stolen or misappropriated. It is not enough to say that a person has accumulated experience and knowledge during the course of his or her employ. Nor can a person be prosecuted on the basis of an assertion that he or she was merely exposed to a trade secret while employed. A prosecution that attempts to tie skill and experience to a particular trade secret should not succeed unless it can show that the particular material was stolen or misappropriated. Thus, the government cannot prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company. Allowing such prosecutions to go forward and allowing the risk of such charges to be brought would unduly endanger legitimate and desirable economic behavior.

As the Pennsylvania Supreme Court noted in *Spring Steels v. Molloy*, 400 Pa. 354, 363 (1960):

"It is not a phenomenal thing in American business life to see an employee, after a long period of service, leave his employment and start a business of his own or in association with others. And it is inevitable in such a situation, where the former employee has dealt with customers on a personal basis that some of those customers will want to continue to deal with him in < that > new association. This is . . . natural, logical and part of human fellowship . . ."

This legislation does not criminalize or in any way hamper these natural incidents of employment. The free and unfettered flow of individuals from one job to another, the ability of a person to start a new business based upon his or her experience and expertise, should not be injured or chilled in any way by this legislation. Individuals must have the opportunity to take advantage of their talents and seeks and accepts other employments that enables them to profit from their abilities and experience. And companies must have the opportunity to employ these people. This measure attempts to safeguard an individual's career mobility and at the same time to preserve the trade secrets that underpin the economic viability of the very company that would offer a person a new job.

The second safeguard is provided by the bill's use of the term "knowingly." For a person to be prosecuted, the person must know or have a firm belief that the information he or she is taking is in fact proprietary. Under theft statutes dealing with tangible property, normally, the thief knows that the object he has stolen is indeed a piece of property that he has no lawful right to convert for his personal use. The same principle applies to this measure-for someone to be convicted under this statute he must be aware or substantially certain that he is misappropriating a trade secret (although a defense should succeed if it is proven that he actually believed that the information was not proprietary after taking reasonable steps to warrant such belief). A person

who takes a trade secret because of ignorance, mistake or accident cannot be prosecuted under the Act.

This requirement should not prove a great barrier to legitimate and warranted prosecutions. Most companies go to considerable pains to protect their trade secrets. Documents are marked proprietary; security measures put in place; and employees often sign confidentiality agreements.

MAINTAINING CONFIDENTIALITY

We have been deeply concerned about the efforts taken by courts to protect the confidentiality of a trade secret. It is important that in the early stages of a prosecution the issue whether material is a trade secret not be litigated. Rather, courts should, when entering these orders, always assume that the material at issue is in fact a trade secret.

VICTIM COMPENSATION

We are also concerned that victims of economic espionage receive compensation for their losses. This legislation incorporates through reference existing law to provide procedures to be used in the detention, seizure, forfeiture, and ultimate disposition of property forfeited under the section. Under these procedures, the Attorney General is authorized to grant petitions for mitigation or remission of forfeiture and for the restoration of forfeited property to the victims of an offense. The Attorney General may also take any other necessary or proper action to protect the rights of innocent people in the interest of justice. In practice, under the forfeiture laws, victims are afforded priority in the disposition of forfeited property since it is the policy of the Department of Justice to provide restitution to the victims of criminal acts whenever permitted to do so by the law. Procedures for victims to obtain restitution may be found at Section 9 of Title 28, Code of Federal Regulations.

In addition to requesting redress from the Attorney General, any person-including a victim-asserting an interest in property ordered forfeited may petition for a judicial hearing to adjudicate the validity of the alleged interest and to revise the order of forfeiture. Additionally, forfeitures are subject to a requirement of proportionality under the Eighth Amendment; that is, the value of the property forfeited must not be excessively disproportionate to the crimes in question.

Finally, we have required that the Attorney General report back to us on victim restitution two and four years after the enactment of this legislation. We have heard from some companies that they only rarely obtain restitution awards despite their eligibility. We wish to carefully monitor restitution to ensure that the current system is working well and make any changes that may be necessary.

FINES PROVISION

In the original Senate version of this measure, we included a provision allowing courts to impose fines of up to twice the value of the trade secret that was stolen. This specific provision

was eliminated because it was unnecessary in light of 18 U.S.C. s3571(d). We have not used the specific exemption available under 18 U.S.C. s3571(e). We, therefore, fully expect that courts will take full advantage of the provision in 18 U.S.C. s3571(d) allowing for fines of up to twice the gain or loss resulting from the theft of trade secrets and that courts will opt for the larger of the fines available under 18 U.S.C. s3571(d) or the fines provisions of this statute.

*S12214 DEPARTMENT OF JUSTICE OVERSIGHT

The Senate version of this measure included a requirement that all prosecutions brought under the statute receive the prior approval of the Attorney General, the Deputy Attorney General or the head of the Department of Justice's Criminal Division. That provision was eliminated in the measure that the House returned to us. We have not reinserted it based on the assurances of the Department of Justice. The Department of Justice will insert a requirement in the U.S. Attorney's Manual that prosecutions continue to be approved and strictly supervised by the Executive Office of the United States Attorney. The Attorney General has written a letter to us to that effect which we will insert into the record. We expect to review all cases brought under this Act in several years to ensure that the requirement is being enforced and to determine if it needs to remain in place.

Mr. HATCH.

Mr. President, I rise in support of H.R. 3723, the Economic Espionage Act of 1996. This bill makes the theft or unlawful appropriation and conversion of " proprietary economic information" a Federal felony. It is an important bill to all of Federal law enforcement, and I encourage my colleagues to support it. In today's technology revolution, the Congress has recognized the need to develop meaningful legislation that has real teeth to stop a burgeoning criminal enterprise. Such enterprise targets the cutting edge research and development of our Nation's industries, often on behalf of a competitor or foreign state. Until now, there has been no meaningful deterrent to such activity. Victims were often forced to resort to State civil remedies as their only redress. I am confident that all of my colleagues will agree that H.R. 3723, a bill which we have crafted and has undergone minor House modification, is a strong and meaningful deterrent to criminals considering engaging in economic espionage.

There is one provision in the bill originally passed by the Senate but deleted from the House which requires clarification. The original bill passed by the Senate contained a provision that required Attorney General approval prior to the initiation of a prosecution under this legislation. The bill returned to the Senate by the House deleted this requirement. It was my intent to attach an amendment to this bill, reinserting the prior authorization requirement. After numerous discussions with administration and industry officials, a compromise has been reached which will allow this bill to be passed by the full Senate as approved by the House.

We have a letter from the Attorney General which memorializes an agreement we have made concerning this prior authorization requirement.

This agreement provides that the Department of Justice shall implement regulations that require that an indictment can be pursued under this legislation only upon the express prior

approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General-Criminal Division. This agreement shall remain in effect for a period of 5 years from enactment. During that timeframe, the Attorney General will be required to report to the Senate or House Judiciary Committees, any prosecutions carried out under this bill which did not receive such prior authorization. It shall also subject the U.S. Attorney or Justice Department official authorizing such prosecution, to appropriate disciplinary sanctions.

I am confident that the Department of Justice will act in good faith and carry out its terms.

I would like to mention three other provisions included in this bill. The first, included as a floor amendment by myself and Senator KOHL, authorizes \$100 million in grants to the Boys and Girls Clubs of America to establish clubs in public housing and other distressed areas across the country. The Boys and Girls Clubs have an outstanding track record of reducing crime and drug use in the communities they serve, and this legislation will help them extend their reach into the communities that need them most.

Second, I am pleased that this bill included another amendment I offered during Senate consideration, transferring to the Attorney General custody of certain Federal inmates hospitalized at St. Elizabeth's hospital. This provision will ensure that these persons, hospitalized because of not guilty by reason on insanity verdicts in Federal courts, receive appropriate care in safe, secure facilities.

Finally, I would like to note that this legislation includes an amended version of technical corrections legislation to fix errors that have, over time, crept into the Federal criminal code. The continued integrity of the criminal laws depends on making these corrections from time to time, and I am pleased that we have addressed this matter here.

For these reasons, I strongly urge all of my colleagues to fully support H.R. 3723.

I ask unanimous consent that the letter I referenced earlier from the Attorney General be printed in the RECORD.

There being no objection, the letter was ordered to be printed in the RECORD, as follows:

DEPARTMENT OF JUSTICE,
OFFICE OF THE ATTORNEY GENERAL,
Washington, DC, October 1, 1996.
Hon. ORRIN G. HATCH,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR CHAIRMAN HATCH: Thank you for your support of the Economic Espionage Act of 1996 ("Act"). The need for this law cannot be understated as it will close significant gaps in federal law, thereby protecting proprietary economic information and the health and competitiveness of the American economy.

The Department shares your concerns that the legislation be implemented in accordance

with the intent of Congress and therefore will require, for a period of five years after implementation of the Act, that the United States may not file a charge under Chapter 90, or use a violation of Chapter 90 as a predicate offense under any other law, without the personal approval of the Attorney General, the Deputy attorney General, or the Assistant Attorney General for the Criminal Division (or the acting official in each of these positions if a position is filled by the Acting official). This requirement will be implemented by published regulation.

Violations of such regulations will be appropriately sanctionable. Any such violations will be reported by the Attorney General to the Senate and House Judiciary Committees.

Once again, thank you for your leadership in this critical area.

Sincerely,

JANET RENO.

APPENDIX P: TABLE OF AUTHORITIES

CASES

<u>Abbott v. United States</u> , 239 F.2d 310 (5th Cir. 1956)	77, 90, 92
<u>Abercrombie & Fitch Co. v. Hunting World, Inc.</u> , 537 F.2d 4 (2d Cir. 1976)	53
<u>Advanced Computer Services v. MAI Systems Corp.</u> , 845 F. Supp. 356 (E.D. Va. 1994)	13
<u>Alfred Bell & Co. v. Catalda Fine Arts, Inc.</u> , 191 F.2d 99 (2d Cir. 1951)	8
<u>Apple Computer, Inc. v. Franklin Computer Corp.</u> , 714 F.2d 1240 (3d Cir. 1983), <u>cert. denied</u> , 464 U.S. 1033 (1984)	6, 9, 13
<u>Apollo Technologies v. Centrosphere Indus.</u> , 805 F. Supp. 1157 (D.N.J. 1992)	75, 76
<u>Atari Games Corp. v. Oman</u> , 888 F.2d 878 (D.C. Cir. 1989)	6, 9
<u>Atari, Inc. v. North American Philips Consumer Elec. Corp.</u> , 672 F.2d 607 (7th Cir.), <u>cert. denied</u> , 459 U.S. 880 (1982)	21
<u>Autoskill Inc. v. National Educational Support Systems, Inc.</u> , 994 F.2d 1476 (10th Cir.), <u>cert. denied</u> , 510 U.S. 916 (1994)	19
<u>Bayer Co. v. United Drug Co.</u> , 272 F. 505 (S.D.N.Y. 1921)	55
<u>Carpenter v. United States</u> , 484 U.S. 19 (1987)	48, 97
<u>Churder v. United States</u> , 387 F.2d 825 (8th Cir. 1968) (18 U.S.C. § 641)	76, 90
<u>Coca-Cola Bottling Co. v. Coca-Cola Co.</u> , 269 F. 796 (3d Cir. 1920)	2
<u>Computer Associates Intern., Inc. v. Altai, Inc.</u> , 982 F.2d 693 (2d Cir. 1992)	21
<u>Cooper v. United States</u> , 639 F. Supp. 176 (M.D. Fla. 1986)	45
<u>Crow v. Wainwright</u> , 720 F.2d 1224 (11th Cir. 1983), <u>cert. denied</u> , 469 U.S. 819 (1984)	6
<u>Daboub v. Gibbons</u> , 42 F.3d 285 (5th Cir. 1995)	6
<u>Dowling v. United States</u> , 473 U.S. 207 (1985)	6, <i>passim</i>
<u>Evans v. Continental Homes, Inc.</u> , 785 F.2d 897 (11th Cir. 1986)	41
<u>Feist Publications Inc. v. Rural Telephone Service Co.</u> , 499 U.S. 340 (1991)	7
<u>Gannett v. Depasquale</u> , 443 U.S. 368 (1979)	83
<u>Gates Rubber Co. V. Bando Chem Indus. Ltd.</u> , 9 F.3d 823 (10th Cir. 1993)	21

<u>Gelles-Widmer Co. v. Milton Bradley Co.</u> , 313 F.2d 143 (7th Cir.), <u>cert. denied</u> , 373 U.S. 913 (1963)	8
<u>Gencraft Homes Inc. v. Sumurdy</u> , 688 F. Supp. 289 (E.D. Tex. 1988)	50
<u>Goldstein v. California</u> , 412 U.S. 546 (1973)	5
<u>Hancock v. Decker</u> , 379 F.2d 552 (5th Cir. 1967)	89
<u>Hoehling v. Universal City Studios, Inc.</u> , 618 F.2d 972 (2d Cir.), <u>cert. denied</u> , 449 U.S. 1040 (1980)	21
<u>Kamar Intern. Inc. v. Russ Berrie & Co.</u> , 657 F.2d 1059 (9th Cir. 1981)	21
<u>Kepner-Tregoe Inc. v. Leadership Software Inc.</u> , 12 F.3d 527, (5th Cir.), <u>cert. denied</u> , __U.S.__, 115 S.Ct. 82 (1994)	11
<u>Kewanee Oil Co. v. Bicron Corp.</u> , 416 U.S. 470 (1974)	75, 81
<u>Kregos v. Associated Press</u> , 937 F.2d 700 (2d Cir.), <u>cert. denied</u> , 510 U.S. 1112 (1994)	8
<u>L. Batlin & Son, Inc. v. Snyder</u> , 536 F.2d 486 (2d Cir.), <u>cert. denied</u> , 429 U.S. 857 (1976)	8
<u>MAI Sys. Corp. v. Peak Computer</u> , 991 F.2d 511 (9th Cir. 1993), <u>cert. denied</u> , 510 U.S. 1033 (1994)	75
<u>McCullock v. Albert E. Price, Inc.</u> , 823 F.2d 316 (9th Cir. 1987)	21
<u>Merritt Forbes & Co. v. Newman Inv. Secs., Inc.</u> , 604 F. Supp. 943, 951 (S.D.N.Y. 1985)	11
<u>Montres Rolex, S.A. v. Snyder</u> , 718 F.2d 524 (2d Cir. 1983), <u>cert. denied</u> , 465 U.S. 1100 (1984)	58
<u>Pioneer Hi-Bred Int'l v. Holden Found. Seeds</u> , 35 F.3d 1226 (8th Cir. 1994)	75
<u>Ratzlaf v. United States</u> , 510 U.S. 135 (1994)	23
<u>Red Baron-Franklin Park v. Taito Corporation</u> , 883 F.2d 275 (4th Cir. 1989), <u>cert. denied</u> , 493 U.S. 1058 (1990)	13, 46
<u>Religious Technology Ctr. v. Netcom On-Line Com.</u> , 923 F. Supp. 1231 (N.D. Cal. 1995)	76
<u>Rivendell Forest Prods. Ltd. v. Georgia-Pacific Corp.</u> , 28 F.3d 1042 (10th Cir. 1994)	75
<u>Rockwell Graphic Sys., Inc. v. DEV Industries, Inc.</u> , 925 F.2d 174 (7th Cir. 1991)	1, 76
<u>Rolex Watch USA, Inc. v. Canner</u> , 645 F. Supp. 484 (S.D. Fla. 1986)	58
<u>Rosciszewski v. Arete Associates, Inc.</u> , 1 F.3d 225 (4th Cir. 1993)	6

<u>Sega Enters. Ltd. v. MAPHIA</u> , 1996 WL 734409 (W.D.Cal. Dec. 18, 1996)	69
<u>Sheldon v. Metro-Goldwin Pictures Corp.</u> , 81 F.2d 49 (2d Cir.), <u>cert. denied</u> , 298 U.S. 669 (1936)	21
<u>Sid & Marty Krofft Television v. McDonald's Corp.</u> , 562 F.2d 1157 (9th Cir. 1977)	8, 21
<u>Sony Corp. v. Universal City Studios, Inc.</u> , 464 U.S. 417 (1984)	7, 10
<u>Spies v. United States</u> , 317 U.S. 492 (1943)	24
<u>Stamicarbon, N.V. v. American Cyanamid Co.</u> , 506 F.2d 532 (2d Cir. 1974)	84
<u>State ex rel. La Crosse Tribune v. Circuit Court</u> , 340 N.W. 2d 460 (Wis. 1983)	84
<u>Systems Corp. v. Peak Computer, Inc.</u> , 991 F.2d 511 (9th Cir.), <u>cert. denied</u> , 510 U.S. 1033 (1994)	13
<u>Taco Cabana Int'l v. Two Pesos, Inc.</u> , 932 F.2d 1113 (5th Cir.), <u>aff'd</u> , 505 U.S. 763 (1992) ..	53
<u>Telerate Sys. Inc. v. Caro</u> , 689 F.Supp. 221 (S.D.N.Y. 1988)	81
<u>Thompson v. Hubbard</u> , 131 U.S. 123 (1989)	7
<u>Trade-Mark Cases</u> , 100 U.S. 82 (1879)	51
<u>Trenton v. Infinity Broadcasting Corp.</u> , 865 F. Supp. 1416 (C.D. Cal. 1994)	11
<u>United States v. Atherton</u> , 561 F.2d 747 (9th Cir. 1977)	27, 29, 30
<u>United States v. Backer</u> , 134 F.2d 533 (2d Cir. 1943)	9, 24
<u>United States v. Baker</u> , 807 F.2d 427 (5th Cir. 1986)	56, 59
<u>United States v. Belmont</u> , 715 F.2d 459 (9th Cir.), <u>cert. denied</u> , 465 U.S. 1022 (1984)	89
<u>United States v. Berg</u> , 710 F.Supp. 438 (E.D.N.Y. 1989)	93
<u>United States v. Berkwitt</u> , 619 F.2d 649, 657 (7th Cir. 1980) (18 U.S.C. § 2311)	77, 90
<u>United States v. Bottone</u> , 365 F.2d 389 (2d Cir.), <u>cert. denied</u> , 385 U.S. 974 (1966) ..	76, 88, 90
<u>United States v. Brown</u> , 925 F.2d 1301 (10th Cir. 1991)	87, 92
<u>United States v. Brumley</u> , 79 F.3d 1430 (5th Cir. 1996)	46, 93
<u>United States v. Caceres</u> , 440 U.S. 741 (1979)	ii
<u>United States v. Cianscewski</u> , 894 F.2d 74 (3rd Cir. 1990)	38, 65
<u>United States v. Cross</u> , 816 F.2d 297, 301 (7th Cir. 1987)	24, 25
<u>United States v. Dixon</u> , 509 U.S. 688, 698 (1993)	68, 86
<u>United States v. Dowling</u> , 739 F.2d 1445 (9th Cir. 1984), <u>rev'd on other grounds</u> ,	

473 U.S. 207 (1985)	46, 87, 89
<u>United States v. Drebin</u> , 557 F.2d 1316 (9th Cir.), <u>cert. denied</u> ,	
436 U.S. 904 (1978)	29, 31, 76, 90
<u>United States v. Drum</u> , 733 F.2d 1503 (11th Cir.), <u>cert. denied</u> , 469 U.S. 1061 (1984)	29, 30, 31
<u>United States v. Gantos</u> , 817 F.2d 41 (8th Cir.), <u>cert. denied</u> , 484 U.S. 860 (1987)	56, 58
<u>United States v. Gonzalez</u> , 630 F. Supp. 894 (S.D. Fla. 1986)	58
<u>United States v. Goss</u> , 803 F.2d 638 (11th Cir. 1986)	27, 29
<u>United States v. Gray</u> , 96 F.3d 769 (5th Cir. 1996)	93
<u>United States v. Gottesman</u> , 724 F.2d 1517 (2d Cir. 1984)	89
<u>United States v. Greenwald</u> , 479 F.2d 320 (6th Cir.), <u>cert. denied</u> ,	
414 U.S. 854 (1973)	76, 89
<u>United States v. Hayes</u> , 800 F. Supp. 1575 (S.D. Ohio 1992), <u>aff'd in part, vacated in part</u> ,	
995 F.2d 1066 (6th Cir. 1993), <u>appeal after remand</u> , 16 F.3d 1222 (6th Cir. 1994)	13
<u>United States v. Hernandez</u> , 952 F.2d 1110 (9th Cir.), <u>cert. denied</u> , 506 U.S. 920 (1992)	39
<u>United States v. Hon</u> , 904 F.2d 803 (2d Cir.), <u>cert. denied</u> ,	
498 U.S. 1069 (1991)	58, 61
<u>United States v. Hux</u> , 940 F.2d 314 (8th Cir. 1991)	13, 19
<u>United States v. Jewell</u> , 532 F.2d 697 (9th Cir.), <u>cert. denied</u> , 426 U.S. 951 (1976)	59
<u>United States v. Johns</u> , 742 F.Supp. 196 (E.D. Pa. 1990)	93
<u>United States v. Kelly</u> , 507 F. Supp. 495 (E.D. Pa. 1981)	93
<u>United States v. Kim</u> , 963 F.2d 65 (5th Cir. 1992)	38, 65
<u>United States v. Koehler</u> , 24 F.3d 867 (6th Cir.1994)	68
<u>United States v. LaMacchia</u> , 871 F. Supp. 535 (D. Mass. 1994)	46, 49
<u>United States v. Larracuenta</u> , 952 F.2d 672 (2d Cir. 1991)	29, 38, 65
<u>United States v. Lester</u> , 282 F.2d 750 (3d Cir.), <u>cert. denied</u> , 364 U.S. 937 (1961)	77, 89, 90
<u>United States v. Lyda</u> , 279 F.2d 461 (5th Cir. 1960)	90
<u>United States v. Lyons</u> , 992 F.2d 1029 (5th Cir. 1993)	90
<u>United States v. McEvoy</u> , 820 F.2d 1170 (11th Cir.), <u>cert.denied</u> ,	
484 U.S. 902 (1987)	58

<u>United States v. McNally</u> , 483 U.S. 350 (1987)	45
<u>United States v. Moore</u> , 604 F.2d 1228 (9th Cir. 1979)	25, 26, 27, 28
<u>United States v. Moran</u> , 757 F. Supp. 1046 (D. Neb. 1991)	24
<u>United States v. Morrison</u> , 844 F.2d 1057 (4th Cir.), <u>cert. denied</u> , 488 U.S. 908 (1988)	82
<u>United States v. O'Reilly</u> , 794 F.2d 613 (11th Cir. 1986)	6, 9, 22
<u>United States v. Oberhardt</u> , 887 F.2d 790 (7th Cir. 1989)	76, 90
<u>United States v. One Sharp Photocopier, Model SF-7750</u> , 771 F. Supp. 980, (D. Minn. 1991)	49
<u>United States v. Payne</u> , 952 F.2d 827 (4th Cir. 1991)	39
<u>United States v. Powell</u> , 701 F.2d 70 (8th Cir. 1983)	22, 29
<u>United States v. Riggs</u> , 739 F.Supp. 414 (N.D. Ill. 1990)	88
<u>United States v. Riggs</u> , 743 F. Supp 556 (N.D. Ill. 1990)	82
<u>United States v. Rowlee</u> , 899 F.2d 1275 (2d Cir.), <u>cert. denied</u> , 498 U.S. 828 (1990)	82
<u>United States v. Sachs</u> , 801 F.2d 839 (6th Cir. 1986)	29, 30, 31
<u>United States v. Sam Goody, Inc.</u> , 506 F. Supp. 380 (E.D.N.Y. 1981)	43
<u>United States v. Schultz</u> , 482 F.2d 1179 (6th Cir. 1973)	43
<u>United States v. Seagraves</u> , 265 F.2d 876 (3d Cir. 1959)	77, 89, 90
<u>United States v. Seidlitz</u> , 589 F.2d 152 (4th Cir.), <u>cert. denied</u> , 441 U.S. 922 (1979)	92
<u>United States v. Shabazz</u> , 724 F.2d 1536 (11th Cir. 1984)	22, 24, 45, 47
<u>United States v. Sheng</u> , 26 F.3d 135 (9th Cir. 1994)	68
<u>United States v. Sheridan</u> , 329 U.S. 379 (1946)	87
<u>United States v. Song</u> , 934 F.2d 105 (7th Cir. 1991)	63
<u>United States v. Steele</u> , 785 F.2d 743 (9th Cir. 1986)	68
<u>United States v. Stegora</u> , 849 F.2d 291 (8th Cir. 1988) (18 U.S.C. § 2314)	76, 77, 89, 90
<u>United States v. Stoneman</u> , 870 F.2d 102 (3rd Cir.), <u>cert. denied</u> _____ 493 U.S. 891 (1989)	48
<u>United States v. Sung</u> , 51 F.3d 92 (7th Cir. 1995)	59, 65
<u>United States v. Taxe</u> , 540 F.2d 961 (9th Cir.), <u>cert. denied</u> ,	

429 U.S. 1040 (1976)	19, 24, 26, 33
<u>United States v. Torkington</u> , 812 F.2d 1347 (11th Cir. 1987)	58
<u>United States v. Turley</u> , 352 U.S. 407, (1957)	90
<u>United States v. Von Banta</u> , 635 F.2d 999 (2d Cir.), <u>cert. denied</u> , 439 U.S. 896 (1978)	92
<u>United States v. Wallington</u> , 889 F.2d 573 (5th Cir. 1989)	94
<u>United States v. Whetzel</u> , 589 F.2d 707 (D.C. Cir. 1978)	30
<u>United States v. Wilson</u> , 900 F.2d 1350 (9th Cir. 1990)	38, 65, 77, 90
<u>United States v. Wise</u> , 550 F.2d 1180 (9th Cir.), <u>cert. denied</u> , 434 U.S. 929 (1977)	19, 24, 25, 29
<u>West Publishing Co. v. Mead Data Central, Inc.</u> , 799 F.2d 1219 (8th Cir. 1986)	8
<u>Whelan Associates, Inc. v. Taslow Dental Library, Inc.</u> , 797 F.2d 1222 (3d Cir. 1986), <u>cert. denied</u> , 479 U.S. 1031 (1987)	13
<u>Williams Electronics, Inc. v. Arctic International, Inc.</u> , 685 F.2d 870 (3d Cir. 1982)	7
<u>United States v. Yamin</u> , 868 F.2d 130 (5th Cir.), <u>cert. denied</u> , 492 U.S. 924 (1989)	56, 58

CONSTITUTIONAL PROVISIONS

U.S. Const. art. I, § 8, cl.3	52
U.S. Const. art. I, § 8, cl.8	5, 11, 51

FEDERAL REGULATIONS

37 C.F.R. § 2.161	55
U.S.S.G. § 1B.5(b)(2)	39
U.S.S.G. § 2B5.1(b)	41
U.S.S.G. § 2F1.1	38, 44

U.S.S.G. § 2F1.1(b)(1)	39
U.S.S.G. § 2F1.1(b)(2)	39
U.S.S.G. § 2F1.1(b)(2)(A)	39
U.S.S.G. § 2F1.1(b)(3)(B)	39

FEDERAL PUBLICATIONS

<u>Federal Guidelines for Searching and Seizing Computers</u> , U.S. Department of Justice, Computer Crime and Intellectual Property Section (1994)	14
<u>Money Laundering Federal Prosecution Manual</u> , U.S. Department of Justice, Money Laundering Section (1994)	35, 61
U.S. Attorney's Manual 9-2.164	31
U.S. Attorney's Manual 9-61.248	91
U.S. Attorney's Manual 9-61.260 - 9-61.261(A-D)	86
U.S. Attorney's Manual 9-61.270	91
U.S. Attorney's Manual 9-68.310	56
U.S. Attorney's Manual 9-68.320	56
U.S. Attorney's Manual 9-68.331	57, 61
U.S. Attorney's Manual 9-68.331(A-G)	57
U.S. Attorney's Manual 9-68.331(D)	53
U.S. Attorney's Manual 9-68.340	58
U.S. Attorney's Manual 9-68.400	59
U.S. Attorney's Manual 9-105.00	36, 61
U.S. Attorney's Manual 9-110.00 <u>et. seq.</u>	36, 61

LEGISLATIVE HISTORY

130 Cong. Rec. H12076, H12078, 98th Cong., 2d Sess. (daily ed. Oct. 10, 1984)	56
142 Cong. Rec. S12201 (daily ed. Oct. 2, 1996)	3, <i>passim</i>
H.R. 104-556, 104th Cong., 2d Sess. (1996)	43
H.R. Rep. No. 788, 104th Cong., 2d Sess. (1996)	78, 79
H.R. Rep. No. 997, 102 Cong., 2d Sess. (1992), reprinted in 1992 U.S. Code Cong. & Admin. News 3569 (1992).	20, 23, 32
H.R. Rep. No. 1476, 94th Cong., 2d Sess. 1, reprinted in 1976 U.S. Code Cong. & Admin News 5659	6
Pub. L. No. 96-517, § 10, 94 Stat. 3028 (1980)	12
Pub. L. No. 97-180, at 8 (1981)	34, 43
Pub. L. No. 102-561, Oct. 28, 1992, 106 Stat. 4233 (amending 18 U.S.C. § 2319)	17, 18
Pub. L. No. 103-322, 108 Stat. 2110, 2148 (1994)	64
Pub. L. No. 103-465 § 513(a), 108 Stat. 4974 (1994)	17, 18, 40
Pub. L. No. 104-153, 110 Stat. 1386 (1996)	43, <i>passim</i>
S Rep. No. 359, 104th Cong., 2d Sess. 16 (1996)	73

STATUTES

15 U.S.C. § 1057	52
15 U.S.C. § 1116	52
15 U.S.C. § 1116(d)	52, 65
15 U.S.C. § 1116(d)(2)	66, 67
15 U.S.C. § 1116(d)(4)(A)	67
15 U.S.C. § 1116(d)(4)(b)(v)	67
15 U.S.C. § 1116(d)(4)(b)(vi)	67
15 U.S.C. § 1116(d)(4)(B)(iii)	66

15 U.S.C. § 1116(d)(4)(B)(iv)	67
15 U.S.C. § 1116(d)(9)	66
15 U.S.C. § 1117	52
15 U.S.C. § 1121	52
15 U.S.C. § 1027	54
15 U.S.C. § 1051 §§§	2, 52, 62, 65
15 U.S.C. § 1051(a)	53
15 U.S.C. § 1051(b)	53
15 U.S.C. § 1052	53
15 U.S.C. § 1127	2
15 U.S.C. § 2320(d)(1)(A)(iii)	57
17 U.S.C. § 101	9, <i>passim</i>
17 U.S.C. § 102(a)	1, 7, 9
17 U.S.C. § 102(b)	10, 22
17 U.S.C. §§ 102(a)(7)	6
17 U.S.C. § 106	2, 11, 20, 27
17 U.S.C. §§ 106 to 120	19
17 U.S.C. § 106(1)	10, 20
17 U.S.C. § 106(3)	15, 20, 27
17 U.S.C. § 106(4)-(5)	20
17 U.S.C. § 107	11, 23
17 U.S.C. § 109	11
17 U.S.C. § 109(a)	27
17 U.S.C. § 109(b)(1)(A)	14
17 U.S.C. § 109(d)	28
17 U.S.C. § 110	22
17 U.S.C. § 115	46
17 U.S.C. § 117	9, 12, 22
17 U.S.C. § 118	22

17 U.S.C. § 201(b)	11
17 U.S.C. § 301	6, 37, 50
17 U.S.C. § 301(a)	6
17 U.S.C. § 302	12
17 U.S.C. § 302(a)	11
17 U.S.C. § 303	11
17 U.S.C. § 304	11
17 U.S.C. § 408	9
17 U.S.C. § 409(1)-(11)	42
17 U.S.C. § 410(c)	10, 19
17 U.S.C. § 411	9
17 U.S.C. § 411(a)	9
17 U.S.C. § 412	9
17 U.S.C. § 501(a)	19, 47
17 U.S.C. § 503(a)	36
17 U.S.C. § 506	6, 7, 13, 38, 47
17 U.S.C. § 506(a)	13, <i>passim</i>
17 U.S.C. § 506(b)	48, 51
17 U.S.C. § 506(c)	4, 17, 41
17 U.S.C. § 506(d)	17, 41
17 U.S.C. § 506(e)	4, 17, 41
17 U.S.C. § 507(a)	47, 68
17 U.S.C. § 509	36, 48
17 U.S.C. § 602	47
17 U.S.C. § 708	9
18 U.S.C. § 371	19, 39, 56, 63
18 U.S.C. § 401	35, 62
18 U.S.C. § 497	4
18 U.S.C. § 506(a)	48

18 U.S.C. § 545	47
18 U.S.C. § 641	77, 82, 90
18 U.S.C. § 1030	94
18 U.S.C. §§ 1030(a)(2)(C)	94
18 U.S.C. § 1030(a)(4)	90, 94
18 U.S.C. § 1052	53
18 U.S.C. § 1116(d)(9)	66
18 U.S.C. § 1341	3, 46, 48, 74, 91
18 U.S.C. § 1343	3, 45, 91
18 U.S.C. § 1346	97, 98
18 U.S.C. § 1831	3, <i>passim</i>
18 U.S.C. § 1832	3, <i>passim</i>
18 U.S.C. §§ 1833	3
18 U.S.C. § 1834	72
18 U.S.C. § 1834(a)(1)	82
18 U.S.C. § 1834(a)(2)	83
18 U.S.C. § 1835	72, 83
18 U.S.C. § 1836	72
18 U.S.C. § 1836(a)	83
18 U.S.C. § 1837	72, 84
18 U.S.C. § 1839	74
18 U.S.C. § 1839(1)	78
18 U.S.C. § 1839(2)	78
18 U.S.C. § 1839(3)(A)	75
18 U.S.C. § 1839(3)(B)	76
18 U.S.C. § 1905	3, 70, 85, 93
18 U.S.C. § 1956	7, 35, 61
18 U.S.C. § 1961(1)(b)	41
18 U.S.C. § 1963	36, 61

18 U.S.C. § 2311	77, 90
18 U.S.C. § 2312	90
18 U.S.C. § 2314	3, <i>passim</i>
18 U.S.C. § 2315	3, 91
18 U.S.C. § 2318	34, <i>passim</i>
18 U.S.C. § 2318(a)	44
18 U.S.C. § 2318(b)(1)	43
18 U.S.C. § 2318(b)(2)	43
18 U.S.C. § 2318(c)(1-4)	44
18 U.S.C. § 2318(d)	48
18 U.S.C. § 2319	7, <i>passim</i>
18 U.S.C. § 2319A	17, 40, 48, 50
18 U.S.C. § 2319A(a)	40, 41
18 U.S.C. § 2319A(b)	41, 48
18 U.S.C. § 2319A(c)	41
18 U.S.C. §§ 2319(b), 3571(b)(3)	37, 38
18 U.S.C. § 2319(b)(1)	20, 31, 37
18 U.S.C. § 2319(b)(3)	21, 31, 37
18 U.S.C. § 2320	ii, <i>passim</i>
18 U.S.C. § 2320(b)	66
18 U.S.C. § 2320(c)	59
18 U.S.C. § 2320(c)(7)(D)	61
18 U.S.C. § 2320(d)(1)	57
18 U.S.C. § 2320(d)(1)(A)(ii)	57
18 U.S.C. § 2320(d)(1)(A)(I)	57
18 U.S.C. § 2320(d)(1)(A)(I), (ii)	57
18 U.S.C. § 2320(d)(2)	56, 68
18 U.S.C. § 2320(e)	49
18 U.S.C. § 3237	91

18 U.S.C. § 3282	50, 68
18 U.S.C. §§ 3571	18
18 U.S.C. §§ 3571(b)(3)	37
18 U.S.C. §§ 3571(b)(5)	37
18 U.S.C. § 5031	36, 63
19 U.S.C. § 1601 et seq.	49
19 U.S.C. § 1615	49
35 U.S.C. § 101.	3
35 U.S.C. § 103	3
35 U.S.C. § 271(a)	3
35 U.S.C. §§ 281-294	4
Act of March 4, 1909, ch. 28, 35 Stat. 1082	5
Act of May 31, 1790, ch. 15, 1 Stat. 124	5

REFERENCE MATERIALS

Paul Goldstein, <u>Copyright's Highway, The Law and Lore of Copyright</u> from <u>Gutenberg to the Celestial Jukebox</u> , 205 (1994)	10
Aaron Hoog, Note, <u>Defrauding the Wire Fraud Statute: United States v. LaMacchia</u> , 8 HarvJ.L. & Tech. 509 (1995)	47
Ronald L. Johnston, <u>Toward an Effective Strategy in Software Copyright Litigation</u> , 19 Rutgers Comp. & Tech. L.J. 91 (1993)	13
Brian J. Kearney, <u>The Trademark Counterfeiting Act of 1984: A Sensible Legislative</u> <u>Response to the Ills of Commercial Counterfeiting</u> , 14 Fordham Urb. L.J. 115, 119-120 (1986)	61
1 J.Thomas McCarthy, <u>McCarthy on Trademarks and Unfair Competition</u> § 3.01[2] (1995)	51
1 Roger Milgrim, <u>Milgrim on Trade Secrets</u> § 1.04 at 1-126	75
2 Roger Milgrim, <u>Milgrim on Trade Secrets</u> § 12.06[2]{c} (1994)	90

3 Melville Nimmer, David Nimmer, <u>Nimmer on Copyright</u> , §13.03[B]	
at 13-69 to -70 (footnotes omitted)	n. 18
James H.A. Pooley, Mark A. Lemley, and Peter J. Toren, <u>Understanding the Economic</u>	
<u>Espionage Act of 1996</u> , 5 Tex. Int. Prop. L.J. 177 (Winter 1997)	70
Kent Walker, <u>Federal Criminal Remedies for the Theft of Intellectual Property</u> , 16 Hastings	
<u>Comm/Ent. L.J.</u> 681 (1994)	4

